KOMMISJONENS GJENNOMFØRINGSBESLUTNING (EU) 2022/254 **2024/EØS/15/29**

av 17. desember 2021

i henhold til europaparlaments- og rådsforordning (EU) nr. 2016/679 med hensyn til tilstrekkelig beskyttelsesnivå for personopplysninger i Republikken Korea i henhold til loven om vern av personopplysninger

[meddelt under nummer C(2021) 9316](*)

EUROPAKOMMISJONEN HAR

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning)([1]), særlig artikkel 45 nr. 3, og

ut fra følgende betraktninger:

1. INNLEDNING

1) Ved forordning (EU) 2016/679 fastsettes det regler for overføring av personopplysninger fra behandlingsansvarlige eller databehandlere i Unionen til tredjeland og internasjonale organisasjoner i den grad slike overføringer omfattes av forordningens virkeområde. Reglene for internasjonale overføringer av personopplysninger er fastsatt i kapittel V (artikkel 44–50) i den forordningen. Strømmen av personopplysninger til og fra land utenfor Den europeiske union er av avgjørende betydning for å øke den internasjonale handelen og det internasjonale samarbeidet, men det beskyttelsesnivået for personopplysninger som sikres i Unionen, må ikke undergraves av overføringer til tredjeland([2]).

2) I henhold til artikkel 45 nr. 3 i forordning (EU) 2016/679 kan Kommisjonen ved hjelp av gjennomføringsrettsakter treffe beslutning om at et tredjeland, et territorium eller en eller flere angitte sektorer i et tredjeland eller en internasjonal organisasjon sikrer et tilstrekkelig beskyttelsesnivå. I henhold til dette vilkåret kan personopplysninger overføres til et tredjeland uten at det er nødvendig å innhente ytterligere godkjenning, som fastsatt i artikkel 45 nr. 1 og betraktning 103 i forordning (EU) 2016/679.

3) Som angitt i artikkel 45 nr. 2 i forordning (EU) 2016/679 skal vedtakelsen av en beslutning om tilstrekkelig beskyttelsesnivå bygge på en omfattende analyse av tredjelandets rettsorden, som omfatter både reglene som gjelder for dataimportører, og begrensningene og garantiene som gjelder offentlige myndigheters tilgang til personopplysninger. I sin vurdering skal Kommisjonen fastslå om det aktuelle tredjelandet sikrer et beskyttelsesnivå som i det vesentlige tilsvarer det som sikres i Den europeiske union (betraktning 104 i forordning (EU) 2016/679). Hvorvidt dette er tilfellet, skal vurderes i henhold til Unionens regelverk, særlig forordning (EU) 2016/679, og rettspraksisen til Den europeiske unions domstol([3]).

(*) Denne unionsrettsakten, kunngjort i EUT L 44 av 24.2.2022, s. 1, er omhandlet i EØS-komiteens beslutning nr. 219/2022 av 8. juli 2022 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester), se EØS-tillegget til *Den europeiske unions tidende* nr. 24 av 23.3.2023, s. 35.

([1]) EUT L 119 av 4.5.2016, s. 1.

([2]) Se betraktning 101 i forordning (EU) 2016/679.

([3]) Se seneste sak C-311/18, Facebook Ireland and Schrems (*Schrems II*), ECLI:EU:C:2020:559.

4) Som presisert av Den europeiske unions domstol kreves det ikke et identisk beskyttelsesnivå([4]). Det betyr særlig at midlene som det aktuelle tredjelandet bruker for å sikre vern av personopplysninger, kan avvike fra de som brukes i Unionen, så lenge de i praksis viser seg å være effektive med henblikk på å sikre et tilstrekkelig beskyttelsesnivå([5]). Standarden for hva som er et tilstrekkelig beskyttelsesnivå, krever derfor ikke at unionsreglene er kopiert punkt for punkt. Det gjelder snarere å avgjøre om det utenlandske systemet som helhet kan gi det beskyttelsesnivået som kreves med hensyn til innholdet i personvernrettighetene og gjennomføringen av, tilsynet med og håndhevingen av disse i praksis([6]). Det europeiske personvernråds referansedokument om tilstrekkelig beskyttelsesnivå, som har som mål å tydeliggjøre denne standarden ytterligere, gir også veiledning på dette området([7]).

5) Kommisjonen har foretatt en grundig analyse av Republikken Koreas rettsorden og praksis. På grunnlag av funnene angitt i betraktning 8–208 konkluderer Kommisjonen med at Republikken Korea sikrer et tilstrekkelig beskyttelsesnivå for personopplysninger som overføres fra en behandlingsansvarlig eller databehandler i Unionen([8]) til enheter (for eksempel fysiske eller juridiske personer, organisasjoner, offentlige institusjoner) i Republikken Korea som omfattes av virkeområdet for loven om vern av personopplysninger (lov nr. 10465 av 29. mars 2011, sist endret ved lov nr. 16930 av 4. februar 2020). Dette omfatter både behandlingsansvarlige og databehandlere (kalt «underleverandører»([9])) i betydningen angitt i forordning (EU) 2016/679. Konstateringen av at beskyttelsesnivået er tilstrekkelig, omfatter ikke behandling av personopplysninger i forbindelse med religiøse organisasjoners misjonsvirksomhet og politiske partiers nominering av kandidater eller behandling av personlige kredittopplysninger i henhold til kredittopplysningsloven utført av behandlingsansvarlige som er underlagt kommisjonen for finansielle tjenesters tilsyn.

6) I denne konklusjonen tas det hensyn til de ytterligere garantiene fastsatt i melding 2021-5 (vedlegg I) og de offisielle redegjørelsene, forsikringene og de forpliktende tilsagnene som den sørkoreanske regjeringen har gitt Kommisjonen (vedlegg II).

7) Denne beslutningen innebærer at overføringer til behandlingsansvarlige og databehandlere i Republikken Korea kan finne sted uten at det er nødvendig å innhente ytterligere godkjenning. Den berører ikke den direkte anvendelsen av forordning (EU) 2016/679 på disse enhetene dersom vilkårene for forordningens geografiske virkeområde fastsatt i artikkel 3 er oppfylt.

2. REGLER FOR BEHANDLING AV PERSONOPPLYSNINGER

2.1 Republikken Koreas ramme for vern av personopplysninger

8) Rettsordenen som regulerer personvern og vern av personopplysninger i Republikken Korea, har sin opprinnelse landets forfatning som ble offentliggjort 17. juli 1948. Selv om retten til vern av personopplysninger ikke er uttrykkelig fastsatt i forfatningen, anerkjennes den likevel som en grunnleggende rettighet som springer ut av den forfatningsmessige retten til menneskeverd og streben etter lykke (artikkel 10), privatliv (artikkel 17) og personvern i forbindelse med kommunikasjon (artikkel 18). Dette er blitt bekreftet av både høyesterett([10]) og forfatningsdomstolen([11]). Begrensninger av grunnleggende rettigheter og friheter (herunder retten til personvern) kan bare innføres ved lov når det er nødvendig av hensyn til den nasjonale sikkerheten eller for å opprettholde lov og orden med henblikk på borgernes velferd, og må ikke berøre det vesentlige innholdet i den aktuelle rettigheten eller friheten (artikkel 37 nr. 2).

([4]) Sak C-362/14, Maximilian Schrems v. Data Protection Commissioner (*Schrems*), ECLI:EU:C:2015:650 nr. 73.

([5]) *Schrems* nr. 74.

([6]) Se Kommisjonens melding til Europaparlamentet og Rådet om utveksling og vern av personopplysninger i en globalisert verden, COM(2017) 7 av 10.1.2017, avsnitt 3.1, s. 6–7.

([7]) Det europeiske personvernråd, Adequacy Referential, WP 254 rev. 01 tilgjengelig på https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108

([8]) Denne beslutningen er relevant for EØS. I henhold til avtalen om Det europeiske økonomiske samarbeidsområde (EØS-avtalen) utvides Den europeiske unions indre marked til å omfatte de tre EØS-statene Island, Liechtenstein og Norge. EØS-komiteens beslutning om innlemming av forordning (EU) 2016/679 i vedlegg XI til EØS-avtalen ble vedtatt av EØS-komiteen 6. juli 2018 og trådte i kraft 20. juli 2018. Forordningen omfattes dermed av nevnte avtale. Med henblikk på beslutningen bør henvisninger til EU og EUs medlemsstater dermed forstås som at de også omfatter EØS-statene.

([9]) Se avsnitt 2.2.3 i denne beslutningen.

([10]) Se for eksempel høyesteretts avgjørelse 2014Da77970 av 15. oktober 2015 (engelsk sammendrag finnes under «Lawmaker's disclosure of teachers' trade union members case» på https://www.privacy.go.kr/eng/enforcement_01.do) og rettspraksisen nevnt der, herunder avgjørelse 2012Da49933 av 24. juli 2014.

([11]) Se særlig forfatningsdomstolens avgjørelse 99Hun-ma513 av 26. mai 2005 (engelsk sammendrag er tilgjengelig på http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) og beslutning 2014JHun-ma449 2013 Hun-Ba68 (konsolidert) av 23. desember 2015 (engelsk sammendrag finnes under «Change of resident registration number case» på https://www.privacy.go.kr/eng/enforcement_01.do).

9) Selv om forfatningen flere steder viser til sørkoreanske statsborgeres rettigheter, har forfatningsdomstolen fastslått at fremmede borgere også har grunnleggende rettigheter([12]). Domstolen har særlig fastslått at vern av ens personlige verdighet og verdi som menneske samt retten til å strebe etter lykke er rettigheter som ethvert menneske har, ikke bare statsborgere([13]). I henhold til den sørkoreanske regjeringens offisielle redegjørelser([14]) er det dessuten allment anerkjent at grunnleggende menneskerettigheter er fastsatt i forfatningens artikkel 12–22 (som omfatter retten til personvern)([15]). Selv om det foreløpig ikke finnes noen rettspraksis som spesifikt gjelder fremmede borgeres rett til personvern, understøtter det faktum at denne retten er forankret i vernet av menneskeverdet og strebenen etter lykke, denne konklusjonen([16]).

10) Republikken Korea har dessuten vedtatt en rekke lover på området vern av personopplysninger som inneholder garantier for alle enkeltpersoner uansett nasjonalitet([17]). I forbindelse med denne beslutningen er følgende lover relevante:

— Loven om vern av personopplysninger (Personal Information Protection Act – PIPA).

— Loven om bruk og vern av kredittopplysninger([18]).

— Loven om personvern i forbindelse med kommunikasjon.

11) PIPA utgjør den generelle rettslige rammen for vern av personopplysninger i Republikken Korea. Den utfylles av et gjennomføringsdekret (presidentdekret nr. 23169 av 29. september 2011, sist endret ved presidentdekret nr. 30892 av 4. august 2020) (heretter kalt «gjennomføringsdekretet til PIPA»), som i likhet med PIPA er rettslig bindende og tvangskraftig.

12) Dessuten inneholder regulatoriske «meldinger» vedtatt av kommisjonen for vern av personopplysninger (Personal Information Protection Commission – PIPC) ytterligere regler for fortolkning og bruk av PIPA. På grunnlag av artikkel 5 (statens forpliktelser) og artikkel 14 (internasjonalt samarbeid) i PIPA har PIPC vedtatt melding 2021-5 av 1. september 2020 (endret ved melding 2021-1 av 21. januar 2021 og melding 2021-5 av 16. november 2021, heretter kalt «melding 2021-5») om fortolkning, anvendelse og håndheving av visse bestemmelser i PIPA. Denne meldingen inneholder presiseringer som får anvendelse på enhver behandling av personopplysninger i henhold til PIPA, samt ytterligere garantier for personopplysninger som overføres til Republikken Korea på grunnlag av denne beslutningen. Meldingen er rettslig bindende for behandlingsansvarlige og kan håndheves av både PIPC og domstolene([19]). En overtredelse av reglene i meldingen innebærer en overtredelse av de relevante bestemmelsene i PIPA som de utfyller. Innholdet i de ytterligere garantiene er derfor analysert som en del av vurderingen av de relevante artiklene i PIPA. Håndboken og retningslinjene for PIPA vedtatt av PIPC([20]) inneholder ytterligere veiledning om PIPA og dens gjennomføringsdekret, som danner grunnlaget for PIPCs anvendelse og håndheving av reglene for vern av personopplysninger.

([12]) Forfatningsdomstolens avgjørelse 93 Hun-MA120 av 29. desember 1994.

([13]) Forfatningsdomstolens avgjørelse 99HeonMa494 av 29. november 2001.

([14]) Se vedlegg II avsnitt 1.1.

([15]) Se også artikkel 1 i loven om vern av personopplysninger der det uttrykkelig vises til «enkeltpersoners friheter og rettigheter». Mer spesifikt angis det at formålet med en slik lov er å «sikre behandling og vern av personopplysninger med henblikk på å verne enkeltpersoners friheter og rettigheter og styrke den enkeltes verdighet og verdi». I artikkel 5 nr. 1 i loven om vern av personopplysninger fastslås det også at staten har ansvar for å «utforme strategier for å hindre skadelige konsekvenser av innsamling som ikke er i henhold til formålet, misbruk og feil bruk av personopplysninger, gjennomgripende overvåking og sporing osv. og for å styrke menneskers verdighet og personvern».

([16]) Videre er det i forfatningens artikkel 6 nr. 2 fastsatt at fremmede borgeres status er garantert i samsvar med folkeretten og internasjonale traktater. Republikken Korea har sluttet seg til en rekke internasjonale avtaler som garanterer retten til personvern, for eksempel den internasjonale konvensjonen om sivile og politiske rettigheter (artikkel 17), konvensjonen om rettighetene til mennesker med nedsatt funksjonsevne (artikkel 22) og konvensjonen om barns rettigheter (artikkel 16).

([17]) Dette omfatter regler som er relevante for vern av personopplysninger, men som ikke får anvendelse i situasjoner der personopplysninger samles inn i Unionen og overføres til Republikken Korea i henhold til forordning (EU) 2016/679, for eksempel i loven om vern, bruk osv. av lokaliseringsopplysninger.

([18]) Formålet med denne loven er å fremme en sunn kredittopplysningsvirksomhet, fremme en effektiv bruk og systematisk håndtering av kredittopplysninger og beskytte personvernet mot misbruk og feil bruk av kredittopplysninger (lovens artikkel 1).

([19]) Republikken Koreas domstoler har for eksempel avgitt kjennelser om overholdelse av regulatoriske meldinger i en rekke saker, herunder ved å holde sørkoreanske behandlingsansvarlige ansvarlige for manglende overholdelse av en melding (se for eksempel høyesteretts avgjørelse 2018Da219406 av 25. oktober 2018, der domstolen påla en behandlingsansvarlig å betale erstatning til enkeltpersoner for skade som følge av manglende overholdelse av «meldingen om standarden for tiltak for å garantere personopplysningers sikkerhet», se også høyesteretts avgjørelse 2018Da219352 av 25. oktober 2018, høyesteretts avgjørelse 2011Da24555 av 16. mai 2016, Seouls sentrale distriktsdomstols avgjørelse 2014Gahap511956 av 13. oktober 2016 og Seouls sentrale distriktsdomstols avgjørelse 2009Gahap43176 av 26. januar 2010).

([20]) Artikkel 12 nr. 1 i PIPA.

13) I tillegg inneholder loven om bruk og vern av kredittopplysninger (Act on the Use and Protection of Credit Information – CIA) særlige regler som gjelder for både «vanlige» kommersielle operatører og spesialiserte enheter i finanssektoren når de behandler personlige kredittopplysninger, det vil si opplysninger som er nødvendige for å fastslå kredittverdigheten til parter i finansielle eller kommersielle transaksjoner. Dette omfatter særlig navn, kontaktopplysninger, finansielle transaksjoner, kredittvurdering, forsikringsstatus eller lånebalanse når slike opplysninger brukes for å fastslå en persons kredittverdighet([21]). Når slike opplysninger brukes for andre formål (for eksempel i forbindelse med personalforvaltning), får PIPA derimot anvendelse i sin helhet. Når det gjelder de spesifikke bestemmelsene i CIA om vern av personopplysninger, kontrolleres overholdelsen dels av PIPC (for kommersielle organisasjoner, se artikkel 45-3 i CIA) og dels av kommisjonen for finansielle tjenester([22]) (for finanssektoren, herunder kredittvurderingsbyråer, banker, forsikringsselskaper, gjensidige sparebanker, spesialiserte kredittfinansieringsselskaper, finansielle investeringsselskaper, verdipapirfinansieringsselskaper, kredittforeninger osv., se artikkel 45 nr. 1 i CIA sammenholdt med artikkel 36-2 i gjennomføringsdekretet til CIA, og artikkel 38 i loven om kommisjonen for finansielle tjenester). I denne forbindelse er virkeområdet for denne beslutningen begrenset til kommersielle operatører som er underlagt PIPCs tilsyn([23]). De spesifikke reglene i CIA som får anvendelse i denne forbindelse (de generelle reglene i PIPA får anvendelse dersom det ikke finnes særlige regler), er beskrevet i avsnitt 2.3.11.

2.2 **PIPAs saklige og personelle virkeområde**

14) Med mindre annet er uttrykkelig fastsatt i andre rettsakter, hører vernet av personopplysninger inn under PIPA (artikkel 6). PIPAs saklige og personelle virkeområde bestemmes av de definerte begrepene «personopplysninger», «behandling» og «behandlingsansvarlig».

2.2.1 *Definisjon av personopplysninger*

15) I artikkel 2 nr. 1 i PIPA defineres personopplysninger som opplysninger om en levende person som identifiserer den personen direkte, for eksempel ved vedkommendes navn, folkeregisternummer eller bilde, eller indirekte, det vil si når opplysninger som i seg selv ikke kan identifisere en bestemt person, lett kan samkjøres med andre opplysninger. Hvorvidt opplysninger «lett» kan samkjøres, avhenger av om en slik samkjøring med rimelighet kan anses som sannsynlig, idet det tas hensyn til muligheten for å innhente andre opplysninger og tiden, kostnadene og teknologien som kreves for å identifisere en person.

16) Pseudonymiserte opplysninger, det vil si opplysninger som ikke kan identifisere en bestemt person uten at de brukes eller samkjøres med andre opplysninger for å gjenopprette opplysningenes opprinnelige form, anses dessuten som personopplysninger i henhold til PIPA (artikkel 2 nr. 1 bokstav c) i PIPA). Opplysninger som er fullt ut «anonymisert», omfattes derimot ikke av PIPAs virkeområde (artikkel 58-2 i PIPA). Dette gjelder opplysninger som ikke kan identifisere en bestemt person, selv om de samkjøres med andre opplysninger, idet det tas hensyn til tiden, kostnaden og teknologien som med rimelighet kreves med henblikk på identifisering.

17) Dette svarer til det saklige virkeområdet for forordning (EU) 2016/679 og forordningens begreper «personopplysninger», «pseudonymisering»([24]) og «anonymiserte opplysninger»([25]).

([21]) Artikkel 2 nr. 1 i CIA.

([22]) Kommisjonen for finansielle tjenester er Republikken Koreas tilsynsmyndighet for finanssektoren og håndhever i egenskap av dette også CIA.

([23]) Dersom dette endres i fremtiden, for eksempel ved å utvide PIPCs kompetanseområde til å omfatte all behandling av personlige kredittopplysninger i henhold til CIA, kan det vurderes å endre beslutningen om tilstrekkelig beskyttelsesnivå, slik at den også omfatter de enhetene som i dag er underlagt kommisjonen for finansielle tjenesters tilsyn.

([24]) I PIPA anses «pseudonymisert behandling» som behandling ved bruk av metoder som delvis sletting av personopplysninger eller delvis eller fullstendig erstatning av personopplysninger på en slik måte at ingen spesifikk person kan gjenkjennes uten supplerende opplysninger (artikkel 2 nr. 1–2 i PIPA). Dette svarer til definisjonen av pseudonymisering i artikkel 4 nr. 5 i forordning (EU) 2016/679, der det vises til «behandling av personopplysninger på en slik måte at personopplysningene ikke lenger kan knyttes til en bestemt registrert uten bruk av tilleggsopplysninger, forutsatt at nevnte tilleggsopplysninger lagres atskilt og omfattes av tekniske og organisatoriske tiltak som sikrer at personopplysningene ikke kan knyttes til en identifisert eller identifiserbar person».

([25]) I betraktning 26 i forordning (EU) 2016/679 presiseres det at forordningen ikke bør få anvendelse på anonyme opplysninger, nærmere bestemt opplysninger som ikke kan knyttes til en identifisert eller identifiserbar fysisk person. Dette avhenger av alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige eller en annen person kan ta i bruk for å identifisere vedkommende direkte eller indirekte. For å fastslå om slike midler med rimelighet kan tenkes å bli tatt bruk, må det tas hensyn til alle objektive faktorer, for eksempel kostnadene for og tiden som er nødvendig for å foreta identifikasjonen, idet det tas hensyn til teknologien som er tilgjengelig på behandlingstidspunktet, og den teknologiske utviklingen.

2.2.2 *Definisjon av behandling*

18) Begrepet «behandling» er gitt en vid definisjon i PIPA og omfatter «innsamling, generering, sammenkobling, sammenfletting, registrering, lagring, oppbevaring, verdiøkende behandling, redigering, gjenfinning, produksjon, korrigering, gjenoppretting, bruk, videreformidling, utlevering og tilintetgjøring av personopplysninger og lignende aktiviteter»([26]). Selv om visse bestemmelser i PIPA bare viser til bestemte typer behandling, for eksempel «bruk», «videreformidling» eller «innsamling»([27]), fortolkes begrepet «bruk» som at det omfatter enhver annen form for behandling enn «innsamling» eller «videreformidling» (til tredjeparter). Denne vide fortolkningen av «bruk» sikrer dermed at det ikke er hull i vernet når det gjelder spesifikke behandlingsaktiviteter. Begrepet behandling svarer derfor til begrepet behandling slik det er definert i forordning (EU) 2016/679.

2.2.3 *Behandlingsansvarlig og «underleverandør»*

19) PIPA får anvendelse på «behandlingsansvarlige». I likhet med forordning (EU) 2016/679 omfatter dette enhver offentlig institusjon, juridisk person, organisasjon eller fysisk person som behandler personopplysninger direkte eller indirekte med henblikk på håndtering av personopplysningsfiler som en del av sin virksomhet([28]). I denne forbindelse menes med «personopplysningsfil» «ett eller flere sett med personopplysninger som er ordnet eller organisert på en systematisk måte i henhold til en bestemt regel med henblikk på enkel tilgang til personopplysningene» (artikkel 2 nr. 4 i PIPA)([29]). Internt plikter den behandlingsansvarlige å gi opplæring til personer som er involvert i behandlingen under vedkommendes ledelse, for eksempel selskapets ledere eller ansatte, og å utøve egnet kontroll og tilsyn (artikkel 28 nr. 1 i PIPA).

20) Det gjelder særlige forpliktelser når en behandlingsansvarlig («utkontrakterende part») utkontrakterer behandlingen av personopplysninger til en tredjepart («underleverandør»). Utkontrakteringen må omfattes av en rettslig bindende ordning (vanligvis en avtale)([30]) som fastsetter omfanget av det utkontrakterte arbeidet, formålet med behandlingen, de tekniske og administrative garantiene som skal gjelde, den behandlingsansvarliges kontroll, erstatningsansvar (for eksempel erstatning for skader som følge av overtredelse av avtaleforpliktelser) og begrensninger for en eventuell underdatabehandling([31]) (artikkel 26 nr. 1 og 2 i PIPA sammenholdt med artikkel 28 nr. 1 i gjennomføringsdekretet)([32]).

21) Den behandlingsansvarlige skal i tillegg offentliggjøre og kontinuerlig oppdatere informasjon om det utkontrakterte arbeidet og underleverandørens identitet eller, i den grad den utkontrakterte behandlingen gjelder aktiviteter knyttet til direkte markedsføring, underrette enkeltpersoner direkte om den relevante informasjonen (artikkel 26 nr. 2 og 3 i PIPA sammenholdt med artikkel 28 nr. 2–5 i gjennomføringsdekretet)([33]).

22) I henhold til artikkel 26 nr. 4 i PIPA sammenholdt med artikkel 28 nr. 6 i gjennomføringsdekretet plikter den behandlingsansvarlige å gi underleverandøren «opplæring» om nødvendige sikkerhetstiltak og å kontrollere, herunder gjennom inspeksjoner, at vedkommende oppfyller alle forpliktelsene som den behandlingsansvarlige har i henhold til PIPA([34]) og avtalen om utkontraktering. Dersom underleverandøren forårsaker skade som følge av en overtredelse av PIPA, gjøres den behandlingsansvarlige ansvarlig for underleverandørens handlinger eller unnlatelse av å handle når det gjelder erstatningsansvar, på samme måte som når det gjelder en ansatt (artikkel 26 nr. 6 i PIPA).

([26]) Artikkel 2 nr. 2 i PIPA.

([27]) Artikkel 15–19 i PIPA viser for eksempel bare til innsamling, bruk og videreformidling av personopplysninger.

([28]) Artikkel 2 nr. 5 i PIPA. I henhold til PIPA omfatter offentlige institusjoner alle sentrale administrative tjenester eller byråer og deres tilknyttede organer, lokale myndigheter, skoler og lokale offentlige selskaper samt nasjonalforsamlingens og rettsvesenets forvaltningsorganer (herunder forfatningsdomstolen) (artikkel 2 nr. 6 i PIPA sammenholdt med artikkel 2 i gjennomføringsdekretet til PIPA).

([29]) Dette svarer til det saklige virkeområde for forordning (EU) 2016/679. I henhold til artikkel 2 nr. i forordning (EU) 2016/679 får forordningen anvendelse på «helt eller delvis automatisert behandling av personopplysninger og på ikke-automatisert behandling av personopplysninger som inngår i eller skal inngå i et register». I artikkel 4 nr. 6 i forordning (EU) 2016/679 defineres «register» som «enhver strukturert samling av personopplysninger som er tilgjengelig etter særlige kriterier.» I tråd med dette forklares det i betraktning 15 at vernet av fysiske personer bør få anvendelse på «automatisert behandling av personopplysninger samt manuell behandling dersom personopplysningene inngår i eller skal inngå i et register. Saksmapper eller samlinger av saksmapper samt deres forsider som ikke er strukturert etter bestemte kriterier, bør ikke omfattes av denne forordnings virkeområde.»

([30]) Se kapittel III avsnitt 2 om artikkel 26 (s. 203–212) i håndboken for PIPA, der det forklares at artikkel 26 nr. 1 i PIPA viser til bindende ordninger, for eksempel avtaler eller lignende ordninger.

([31]) I henhold til artikkel 26 nr. 5 i PIPA er det forbudt for databehandleren å bruke personopplysninger som ikke omfattes av det utkontrakterte arbeidet, eller å utlevere personopplysninger til en tredjepart. Dersom dette kravet ikke oppfylles, kan det føre til strafferettslige sanksjoner i henhold til artikkel 71 pkt. 2 i PIPA.

([32]) Dersom dette kravet ikke oppfylles, kan det føre til ilegging av bøter, se artikkel 75 nr. 4 pkt. 4 i PIPA.

([33]) Dersom dette kravet ikke oppfylles, kan det føre til ilegging av bøter, se artikkel 75 nr. 2 pkt. 1 og nr. 4 pkt. 5 i PIPA.

([34]) Se også artikkel 26 nr. 7 i PIPA der det er fastsatt at artikkel 15–25, artikkel 27–31, artikkel 33–38 og artikkel 50 gjelder tilsvarende med nødvendige endringer for databehandleren.

23) Selv om det i PIPA derfor ikke brukes forskjellige begreper for «behandlingsansvarlige» og «databehandlere», omfatter reglene for utkontraktering i all hovedsak de samme forpliktelsene og garantiene som de som regulerer forholdet mellom behandlingsansvarlige og databehandlere i henhold til forordning (EU) 2016/679.

2.2.4 *Særlige bestemmelser for leverandører av informasjons- og kommunikasjonstjenester*

24) Selv om PIPA får anvendelse på alle behandlingsansvarliges behandling av personopplysninger, inneholder visse bestemmelser særlige regler (som *lex specialis*) for behandling av «brukeres» personopplysninger som utføres av «leverandører av informasjons- og kommunikasjonstjenester»([35]). Begrepet «brukere» omfatter personer som bruker informasjons- og kommunikasjonstjenester (artikkel 2 nr. 1 pkt. 4 i loven om fremming av bruken av informasjons- og kommunikasjonsnettverk og vern av opplysninger, heretter kalt «nettverksloven»). Dette krever at personen enten bruker telekommunikasjonstjenester som leveres av en sørkoreansk teleoperatør, direkte, eller bruker informasjonstjenester([36]) som leveres kommersielt (det vil si med gevinst for øye) av en enhet som bruker tjenester fra en teleoperatør som har lisens / er registrert i Republikken Korea([37]). I begge tilfeller er enheten som er bundet av de særlige bestemmelsene i PIPA, en enhet som tilbyr en nettbasert tjeneste direkte til en person (det vil si en bruker).

25) En konstatering av tilstrekkelig beskyttelsesnivå gjelder imidlertid utelukkende det beskyttelsesnivået som gis personopplysninger som overføres fra en behandlingsansvarlig/databehandler i Unionen, til en enhet i et tredjeland (her Republikken Korea). I sistnevnte scenario vil enkeltpersoner i Unionen normalt bare ha en direkte relasjon til «dataeksportøren» i Unionen og ikke til sørkoreanske leverandører av informasjons- og kommunikasjonstjenester([38]). De særlige bestemmelsene i PIPA som gjelder personopplysninger om brukere av informasjons- og kommunikasjonstjenester, vil derfor bare i begrensede tilfeller få anvendelse på personopplysninger som overføres i henhold til denne beslutningen.

2.2.5 *Unntak fra visse bestemmelser i PIPA*

26) I henhold til artikkel 58 nr. 1 i PIPA får deler av PIPA (det vil si artikkel 15–57) ikke anvendelse på fire kategorier av databehandling([39]). De delene av PIPA som omhandler de spesifikke grunnene til behandling, visse forpliktelser som gjelder vern av opplysninger, de nærmere reglene for utøvelse av individuelle rettigheter og reglene for tvisteløsning via utvalget for tvisteløsning i forbindelse med personopplysninger får ikke anvendelse. Andre grunnleggende bestemmelser i PIPA får fortsatt anvendelse, særlig de generelle bestemmelsene om prinsipper for vern av opplysninger (artikkel 3 i PIPA), herunder for eksempel prinsippene om lovlighet, spesifisering av formål og formålsbegrensning, dataminimering, opplysningenes riktighet og sikkerhet, og individuelle rettigheter (innsyn, retting, sletting og innstilling av behandlingen, se artikkel 4 i PIPA). Ved artikkel 58 nr. 4 i PIPA innføres det også særlige forpliktelser i forbindelse med disse behandlingsaktivitetene, særlig med hensyn til dataminimering, lagringsbegrensning, sikkerhetstiltak og behandling av klager([40]). Som følge av dette kan enkeltpersoner fremdeles klage til PIPC dersom disse prinsippene og forpliktelsene ikke overholdes, og PIPC har myndighet til å treffe håndhevingstiltak ved manglende overholdelse.

([35]) Se særlig artikkel 18 nr. 2 og kapittel VI i PIPA.

([36]) Informasjonstjenester omfatter både levering av informasjons- og formidlingstjenester for levering av informasjon.

([37]) Se artikkel 2 nr. 1 pkt. 3 (sammenholdt med artikkel 2 nr. 1 pkt. 2 og 4) i nettverksloven og artikkel 2 nr. 6 og 8 i loven om telekommunikasjonsvirksomhet.

([38]) I den grad sørkoreanske leverandører av informasjons- og kommunikasjonstjenester har en direkte relasjon til enkeltpersoner i EU (ved å tilby nettbaserte tjenester), kan dette føre til direkte anvendelse av forordning (EU) 2016/679 i henhold til dens artikkel 3 nr. 2 bokstav a).

([39]) I artikkel 58 nr. 2 i PIPA er det videre fastsatt at artikkel 15 og 22, artikkel 27 nr. 1 og 2 og artikkel 34 og 37 ikke får anvendelse på personopplysninger som behandles ved hjelp av utstyr til behandling av visuelle data som installeres og drives på åpne steder. Ettersom denne bestemmelsen gjelder bruken av videoovervåking i Republikken Korea, det vil si direkte innsamling av personopplysninger fra enkeltpersoner i Republikken Korea, er den ikke relevant for denne beslutningen som omfatter overføring av personopplysninger fra behandlingsansvarlige/databehandlere i EU til enheter i Republikken Korea. I henhold til artikkel 58 nr. 3 i PIPA får artikkel 15 (innsamling og bruk av personopplysninger), artikkel 30 (plikt til å innføre en offentlig personvernpolitikk) og artikkel 31 (plikt til å utpeke en personvernansvarlig) ikke anvendelse på personopplysninger som behandles for å drive vennskapsgrupper eller -foreninger (for eksempel hobbyklubber). Ettersom slike grupper anses for å være av personlig art uten tilknytning til en yrkesmessig eller kommersiell aktivitet kreves det ikke et spesifikt rettslig grunnlag (for eksempel samtykke fra de berørte personene) for å samle inn og bruke deres opplysninger i denne sammenhengen. Alle andre bestemmelser i PIPA (for eksempel om dataminimering, formålsbegrensning, behandlingens lovlighet, sikkerhet og individuelle rettigheter) får imidlertid fortsatt anvendelse. Dessuten omfattes enhver behandling av personopplysninger utover det formålet å opprette en sosial gruppe ikke av unntaket.

([40]) I artikkel 58 nr. 4 i PIPA er det mer spesifikt fastsatt at personopplysninger skal behandles i så lite omfang som nødvendig for å oppfylle det tiltenkte formålet, at de skal behandles i kortest mulig tid, og at det skal treffe nødvendige tiltak for å sikre en sikker håndtering og egnet behandling av slike personopplysninger. Det sistnevnte omfatter tekniske, organisatoriske og fysiske garantier samt tiltak for å sikre egnet behandling av individuelle klager.

27) For det første omfatter det delvise unntaket personopplysninger som samles inn i henhold til statistikkloven for å bli behandlet av offentlige institusjoner. I henhold til presiseringer mottatt fra den sørkoreanske regjeringen gjelder personopplysninger som behandles i denne sammenhengen, vanligvis sørkoreanske statsborgere og omfatter bare unntaksvis opplysninger om utlendinger, særlig i forbindelse med statistikk om innreise til og utreise fra territoriet, eller om utenlandske investeringer. Men også i disse situasjonene overføres slike opplysninger vanligvis ikke fra behandlingsansvarlige/databehandlere i Unionen, men samles inn direkte av sørkoreanske offentlige myndigheter([41]). I likhet med det som er fastsatt i betraktning 162 i forordning (EU) 2016/679, er behandling av opplysninger i henhold til statistikkloven dessuten underlagt en rekke vilkår og garantier. Ved statistikkloven er det fastsatt spesifikke forpliktelser, for eksempel for å sikre riktighet, konsistens og upartiskhet, garantere enkeltpersoners rett til konfidensialitet, verne opplysningene til personer som svarer på statistiske undersøkelser, herunder for å hindre at slike opplysninger brukes for andre formål enn utarbeiding av statistikk, og krav til konfidensialitet for ansatte([42]). Offentlige myndigheter som behandler statistikk, må også blant annet overholde prinsippene om dataminimering, formålsbegrensning og sikkerhet (artikkel 3 og artikkel 58 nr. 4 i PIPA) og gi enkeltpersoner mulighet til å utøve sine rettigheter (innsyn, retting, sletting og innstilling av behandlingen, se artikkel 4 i PIPA). Opplysningene må også behandles i anonymisert eller pseudonymisert form dersom dette gjør det mulig å oppfylle formålet med behandlingen (artikkel 3 nr. 7 i PIPA).

28) For det andre viser artikkel 58 nr. 1 i PIPA til personopplysninger som samles inn eller som det anmodes om med henblikk på analysering av opplysninger knyttet nasjonal sikkerhet. Virkeområdet for og konsekvensene av dette delvise unntaket beskrives nærmere i betraktning 149.

29) For det tredje får det delvise unntaket anvendelse på midlertidig behandling av personopplysninger dersom dette er tvingende nødvendig av hensyn til den offentlige sikkerheten, herunder folkehelsen. Denne kategorien fortolkes strengt av PIPC og har i henhold til den mottatte informasjonen aldri blitt brukt. Unntaket får bare anvendelse i nødssituasjoner som krever umiddelbare tiltak, for eksempel for å spore smittestoffer eller for å berge og hjelpe ofre for naturkatastrofer([43]). Selv i disse situasjonene omfatter det delvise unntaket bare behandling av personopplysninger i et begrenset tidsrom for å kunne gjennomføre slike tiltak. Situasjoner der dette kan få anvendelse på overføring av opplysninger som omfattes av denne beslutningen, er enda mer begrenset med tanke på den lave sannsynligheten for at personopplysninger som overføres fra Unionen til sørkoreanske operatører, vil være av den typen som kan gjøre den etterfølgende behandlingen «tvingende nødvendig» i slike nødssituasjoner.

30) For det fjerde får det delvise unntaket anvendelse på personopplysninger som samles inn eller brukes av pressen, i forbindelse med religiøse organisasjoners misjonsvirksomhet eller politiske partiers nominering av kandidater. Unntaket får bare anvendelse når personopplysninger behandles av pressen, religiøse organisasjoner eller politiske partier for disse spesifikke formålene (det vil si journalistisk virksomhet, misjonsvirksomhet og nominering av politiske kandidater). Dersom disse enhetene behandler personopplysninger for andre formål, for eksempel i forbindelse med personalforvaltning eller intern administrasjon, får PIPA full anvendelse.

31) Når det gjelder pressens behandling av personopplysninger i forbindelse med journalistisk virksomhet, er balansen mellom ytringsfrihet og andre rettigheter (herunder retten til personvern) fastsatt i loven om voldgift og rettsmidler osv. ved skade forårsaket av artikler i pressen (heretter kalt «presseloven»)([44]). I artikkel 5 i presseloven er det særlig fastsatt

([41]) I denne forbindelse kreves det i artikkel 33 i statistikkloven at offentlige institusjoner skal beskytte opplysninger fra respondenter som deltar i statistiske undersøkelser, herunder for å hindre at slike opplysninger blir brukt for andre formål enn utarbeiding av statistikk.

([42]) Artikkel 2 nr. 2–3, artikkel 30 nr. 2 og artikkel 33 og 34 i statistikkloven.

([43]) Håndboken for PIPA, avsnittet om artikkel 58.

([44]) I artikkel 4 i presseloven er det for eksempel fastsatt at artikler i pressen skal være upartiske og objektive, i allmennhetens interesse og respektere menneskers verdighet og verdi, og at de verken må ærekrenke andre personer eller krenke deres rettigheter, den offentlige moral eller den sosiale etikk.

at pressen (det vil si kringkastingsforetak, aviser, tidsskrifter eller nettaviser) og nettbaserte nyhetstjenester eller nettbaserte multimedieforetak ikke må krenke den enkeltes personvern. Dersom det likevel skjer en krenking av personvernet, må det straks treffes korrigerende tiltak i samsvar med de spesifikke framgangsmåtene fastsatt i loven. I denne forbindelse gir loven enkeltpersoner som lider skade på grunn av en artikkel i pressen, en rekke rettigheter, for eksempel til å få offentliggjort en retting av et feilaktig utsagn, å utøve en rett til tilsvar eller å få offentliggjort en ny artikkel (dersom en artikkel gjelder påstander om straffbare forhold som den aktuelle personen senere frikjennes for)([45]). Enkeltpersoners krav kan behandles direkte av presseorganene (via et ombud)([46]), ved forlik eller voldgift (ved en voldgiftskommisjon spesialisert på pressespørsmål)([47]) eller ved domstolene. Enkeltpersoner kan også få erstatning dersom de lider økonomisk tap, dersom deres personvern krenkes, eller dersom de lider psykisk overlast som følge av en ulovlig handling fra pressens side (forsettlig eller uaktsom)([48]). Pressen er fritatt for ansvar i henhold til loven dersom en presseartikkel som griper inn i en persons rettigheter, ikke er i strid med sosiale verdier og offentliggjøres enten med den berørte personens samtykke eller i allmennhetens interesse (og det foreligger tilstrekkelige grunner til å anta at artikkelen er sannferdig)([49]).

32) Selv om pressens behandling av personopplysninger i forbindelse med journalistisk virksomhet dermed er underlagt spesifikke garantier i henhold til presseloven, finnes det ingen slike ytterligere garantier for anvendelse av unntakene i forbindelse med religiøse organisasjoners og politiske partiers behandlingsaktiviteter som kan sammenlignes med artikkel 85, 89 og 91 i forordning (EU) 2016/679. Kommisjonen finner det derfor hensiktsmessig at religiøse organisasjoners behandling av personopplysninger i forbindelse med misjonsvirksomhet og politiske partiers behandling av personopplysninger i forbindelse med nominering av kandidater unntas fra denne beslutningens virkeområde.

2.3 **Garantier, rettigheter og forpliktelser**

2.3.1 *Lovlig og rettferdig behandling*

33) Personopplysninger bør behandles på en lovlig og rettferdig måte.

34) Dette prinsippet er fastsatt i artikkel 3 nr. 1 og 2 i PIPA og styrkes av artikkel 59 i PIPA som forbyr behandling av personopplysninger «ved bruk av bedragerske, utilbørlige eller urimelige midler», «uten rettslig myndighet» eller «uten behørig myndighet»([50]). Disse generelle prinsippene for lovlig behandling beskrives nærmere i artikkel 15–19 i PIPA, der de forskjellige rettslige grunnene for behandling (innsamling, bruk og videreformidling til tredjeparter), herunder under hvilke omstendigheter dette kan medføre en endring av formålet (artikkel 18 i PIPA), er fastsatt.

([45]) Artikkel 15–17 i presseloven.

([46]) Hvert presse- eller medieorgan må ha sitt eget ombud for å hindre og avhjelpe eventuelle skader forårsaket av pressen (for eksempel ved å anbefale korrigering av presseartikler som er usanne, eller som skader andres omdømme), se artikkel 6 i presseloven.

([47]) Kommisjonen består av mellom 40 og 90 voldgiftsmenn som ministeren for kultur, idrett og turisme har utpekt blant dommere, advokater eller personer som har arbeidet med nyhetsinnsamling eller -rapportering i minst ti år, eller andre personer med ekspertise på presseområdet. Voldgiftsmenn kan ikke samtidig være offentlige tjenestemenn, medlemmer av politiske partier eller journalister. I samsvar med artikkel 8 i presseloven må voldgiftsmennene utføre sine oppgaver på en uavhengig måte og skal ikke styres eller motta instruksjoner i forbindelse med disse oppgavene. Det finnes dessuten særlige regler for å hindre interessekonflikter, for eksempel ved at individuelle voldgiftsmenn ikke kan håndtere individuelle saker dersom deres ektefelle eller slektninger er part i saken (artikkel 10 i presseloven). Kommisjonen kan løse tvister gjennom forlik eller voldgift, men kan også framsette anbefalinger for å avhjelpe overtredelser (avsnitt 5 i presseloven).

([48]) Artikkel 30 i presseloven.

([49]) Artikkel 5 i presseloven.

([50]) I henhold til artikkel 59 i PIPA forbys personer «som behandler, eller som på noe tidspunkt har behandlet personopplysninger», å «innhente personopplysninger eller samtykke til behandling av personopplysninger ved bruk av bedragerske, utilbørlige eller urimelige midler», «utlevere personopplysninger som er innhentet i forbindelse med yrkesvirksomhet, eller utlevere dem til tredjeparter som ikke har myndighet for dette formålet» eller «skade, tilintetgjøre, endre, forfalske eller utlevere andre personopplysninger uten rettslig myndighet eller uten behørig myndighet». En overtredelse av dette forbudet kan føre til strafferettslige sanksjoner, se artikkel 71 nr. 5 og 6 og artikkel 72 nr. 2 i PIPA. I henhold til artikkel 70 nr. 2 i PIPA er det dessuten mulig å ilegge en strafferettslig sanksjon for innhenting av personopplysninger som er behandlet av tredjeparter, ved bruk av bedragerske eller andre urimelige midler eller metoder eller for å utlevere dem til en tredjepart for vinningsformål eller urimelige formål samt for å oppmuntre til eller organisere en slik atferd.

35) I henhold til artikkel 15 nr. 1 i PIPA kan en behandlingsansvarlig bare samle inn personopplysninger (innenfor rammen av formålet med innsamlingen) i henhold til et begrenset antall rettslige grunner. Disse er 1) den registrertes samtykke([51]) (pkt. 1), 2) behovet for å gjennomføre og oppfylle en avtale med den registrerte (pkt. 4), 3) en spesiell lovbestemt tillatelse eller behovet for å oppfylle en rettslig forpliktelse (pkt. 2), en offentlig institusjons behov([52]) for å utføre oppgavene som hører inn under dens rettslige kompetanse, 4) et åpenbart behov for å beskytte den registrertes eller en tredjeparts liv, legeme eller eiendomsinteresser mot overhengende fare (bare dersom den registrerte ikke er i stand til å uttrykke sin mening, eller dersom det ikke er mulig å innhente samtykke på forhånd) (pkt. 5), 5) behovet for å beskytte den behandlingsansvarliges «berettigede interesse» dersom den «klart går foran» den registrertes interesser (og bare dersom behandlingen har en «vesentlig kobling» til den berettigede interessen og ikke går videre enn det som er rimelig) (pkt. 6)([53]). Disse grunnene til behandling tilsvarer i det vesentlige de som er fastsatt i artikkel 6 i forordning (EU) 2016/679, herunder grunnen «berettiget interesse» i artikkel 6 nr. 1 bokstav f) i forordning (EU) 2016/679.

36) Innsamlede personopplysninger kan brukes innenfor rammen av formålet med innsamlingen (artikkel 15 nr. 1 i PIPA) eller «innenfor rammer som er rimelig relatert» til formålet med innsamlingen, idet det tas hensyn til mulige ulemper for den registrerte, og forutsatt at nødvendige sikkerhetstiltak (for eksempel kryptering) er truffet (artikkel 15 nr. 3 i PIPA). For å fastslå om formålet med bruken er «rimelig relatert» til det opprinnelige formålet med innsamlingen, er det i gjennomføringsdekretet fastsatt spesifikke kriterier som svarer til kriteriene i artikkel 6 nr. 4 i forordning (EU) 2016/679. Det må særlige foreligge en betydelig relevans i forhold til det opprinnelige formålet, den videre bruken må være forutsigbar (for eksempel i lys av omstendighetene som opplysningene ble samlet inn under), og om mulig må opplysningene pseudonymiseres([54]). De spesifikke kriteriene som en behandlingsansvarlig bruker i forbindelse med denne vurderingen, må offentliggjøres på forhånd i personvernprogrammet([55]). Videre er den personvernansvarlige (se betraktning 94) spesifikt forpliktet til å undersøke om den videre bruken skjer innenfor disse parametrene.

([51]) Samtykke skal gis frivillig, det skal være informert, spesifikt og uttrykt på en av flere måter som er fastsatt ved lov. Samtykke kan ikke under noen omstendigheter innhentes ved bruk av bedragerske, utilbørlige eller på andre måter urimelige midler (artikkel 59 nr. 1 i PIPA). For det første har de registrerte i henhold til artikkel 4 pkt. 2 i PIPA rett til «å gi eller nekte å gi samtykke» og til «å definere samtykkets omfang», og bør informeres om dette (artikkel 15 nr. 2, artikkel 16 nr. 2 og 3, artikkel 17 nr. 2 og artikkel 18 nr. 3 i PIPA). Artikkel 22 nr. 5 i PIPA inneholder en supplerende garanti ved at behandlingsansvarlige forbys å nekte levering av varer eller tjenester dersom dette kan undergrave den enkeltes frie valg med hensyn til å gi samtykke. Dette omfatter situasjoner der bare visse typer behandling krever samtykke (mens andre er basert på avtaler), og omfatter også videre behandling av personopplysninger som er samlet inn i forbindelse med levering av varer eller tjenester. For det andre må den behandlingsansvarlige i henhold til artikkel 15 nr. 2, artikkel 17 nr. 2 og 3 og artikkel 18 nr. 3 i PIPA når det bes om samtykke, informere den registrerte om de aktuelle personopplysningenes «særlige art» (for eksempel at det dreier seg om sensitive opplysninger, se artikkel 17 nr. 2 pkt. 2 bokstav a) i gjennomføringsdekretet til PIPA), formålet med behandlingen, lagringstiden og eventuelle mottakere av opplysningene. Alle slike anmodninger skal framsettes «på en tydelig gjenkjennelig måte» der det skilles mellom saker som krever samtykke, og andre (artikkel 22 nr. 1–4 i PIPA). For det tredje angis de spesifikke metodene som en behandlingsansvarlig skal bruke for å innhente samtykke, for eksempel skriftlig samtykke med den registrertes underskrift eller samtykke ved (returnering) av e-post, i artikkel 17 nr. 1 pkt. 1–6 i gjennomføringsdekretet til PIPA. Selv om PIPA ikke spesifikt gir enkeltpersoner en generell rett til å trekke tilbake sitt samtykke, har enkeltpersoner rett til å få innstilt behandlingen av personopplysninger som gjelder dem, og når denne retten utøves, innstilles behandlingen og opplysningene slettes (se betraktning 78 om retten til å få innstilt behandlingen).

([52]) I henhold til informasjon fra PIPC kan offentlige institusjoner bare påberope seg denne grunnen dersom behandlingen av personopplysninger er uunngåelig, det vil si at det må være umulig eller urimelig vanskelig for institusjonen å utføre sine oppgaver uten å behandle opplysningene.

([53]) Ved artikkel 39-3 i PIPA pålegges leverandører av informasjons- og kommunikasjonstjenester spesifikke (strengere) forpliktelser med hensyn til innsamling og bruk av personopplysninger om deres brukere. Det kreves særlig at leverandøren innhenter brukerens samtykke etter å ha gitt informasjon om formålet med innsamlingen/bruken, kategoriene av personopplysninger som skal samles inn, og i hvilket tidsrom opplysningene vil bli behandlet (artikkel 39-3 nr. 1 i PIPA). Det samme gjelder når noen av disse aspektene endres. Manglende innhenting av samtykke til innsamling av opplysninger omfattes av strafferettslige sanksjoner (artikkel 71 nr. 4–5 i PIPA). Brukernes personopplysninger kan unntaksvis samles inn eller brukes av leverandører av informasjons- og kommunikasjonstjenester uten forutgående samtykke. Dette er tilfellet 1) når det av økonomiske og teknologiske grunner er åpenbart vanskelig å innhente normalt samtykke for de personopplysningene som er nødvendige for å gjennomføre avtalen om levering av informasjons- og kommunikasjonstjenester (for eksempel når det uunngåelig opprettes personopplysninger i forbindelse med gjennomføringen av en avtale, for eksempel faktureringsinformasjon, tilgangslogger og betalingsoversikter), 2) når det er nødvendig for betaling av gebyrer etter levering av informasjons- og kommunikasjonstjenester, eller 3) dersom det er tillatt i henhold til andre lover (i artikkel 21 nr. 1 pkt. 6 i loven om forbrukervern ved elektronisk handel er det for eksempel fastsatt at økonomiske operatører kan samle inn personopplysninger om verger for en mindreårig for å bekrefte om det er oppnådd gyldig samtykke på vegne av den mindreårige) (artikkel 39-3 nr. 2 i PIPA). Leverandører av informasjons- og kommunikasjonstjenester kan ikke nekte å levere tjenester bare fordi brukeren ikke gir flere personopplysninger enn det minimum som kreves (det vil si de opplysningene som er nødvendige for å utføre de vesentlige elementene i den aktuelle tjenesten), se artikkel 39-3 nr. 3 i PIPA.

([54]) Se artikkel 14 nr. 2 i gjennomføringsdekretet til PIPA.

([55]) Artikkel 14-2 nr. 2 i gjennomføringsdekretet til PIPA.

37) Det gjelder lignende (men noe strengere) regler for videreformidling av opplysninger til en tredjepart. I henhold til artikkel 17 nr. 1 i PIPA er videreformidling av personopplysninger til en tredjepart tillatt etter samtykke([56]) eller, innenfor rammen av formålet med innsamlingen, dersom opplysningene er blitt samlet inn i henhold til en av de rettslige grunnene i artikkel 15 nr. 1 pkt. 2, 3 og 4 i PIPA. Dette utelukker særlig enhver utlevering basert på den behandlingsansvarliges «berettigede interesse». Utover dette tillater artikkel 17 nr. 4 i PIPA videreformidling til en tredjepart «innenfor rammer som er rimelig relatert» til formålet med innsamlingen, idet det tas hensyn til mulige ulemper for den registrerte, og forutsatt at nødvendige sikkerhetstiltak (for eksempel kryptering) er truffet. Det må tas hensyn til de samme faktorene som de som er beskrevet i betraktning 36, for å vurdere om videreformidlingen er innenfor rammer som er rimelig relatert til formålet med innsamlingen, og de samme garantiene (det vil si med hensyn til åpenhet gjennom personvernprogrammet og den personvernansvarliges medvirkning) får anvendelse.

38) Dersom en sørkoreansk behandlingsansvarlig mottar personopplysninger fra Unionen, anses det som «innsamling» i henhold til artikkel 15 i PIPA. I melding 2021-5 (avsnitt I i vedlegg I til denne beslutningen) presiseres det at formålet som opplysningene ble overført av den berørte EU-enheten for, er den sørkoreanske behandlingsansvarliges formål med innsamlingen. Som følge av dette plikter sørkoreanske behandlingsansvarlige som mottar personopplysninger fra Unionen, i prinsippet å behandle slike opplysninger innenfor rammen av formålet med overføringen i samsvar med artikkel 17 i PIPA.

39) Det gjelder særlige begrensninger dersom den behandlingsansvarlige ønsker å bruke personopplysningene eller videreformidle dem til en tredjepart for et annet formål enn formålet med innsamlingen([57]). I henhold til artikkel 18 nr. 2 i PIPA kan en privat behandlingsansvarlig unntaksvis([58]) bruke personopplysninger eller videreformidle dem til en tredjepart for et annet formål 1) basert på et nytt (det vil si separat) samtykke fra den registrerte, 2) dersom det er fastsatt i særlige lovbestemmelser, eller 3) dersom det foreligger et åpenbart behov for å beskytte den registrertes eller en tredjeparts liv, legeme eller eiendomsinteresser mot overhengende fare (bare dersom den registrerte ikke er i stand til å uttrykke sin mening, og dersom det ikke er mulig å innhente samtykke på forhånd)([59]).

40) I visse situasjoner kan offentlige institusjoner også bruke personopplysninger eller videreformidle dem til en tredjepart for et annet formål. Dette omfatter tilfeller der det ellers ville vært umulig for offentlige institusjoner å utføre sine lovfestede oppgaver, forutsatt at PIPC gir sin godkjenning. Offentlige institusjoner kan dessuten videreformidle personopplysninger til en annen myndighet eller domstol dersom dette er nødvendig for å etterforske og rettsforfølge straffbare forhold eller for å reise tiltale, for at en domstol skal kunne utføre sine oppgaver i forbindelse med en pågående rettergang, eller for å fullbyrde en strafferettslig sanksjon, en beslutning om omsorgsovertakelse eller en fengslingskjennelse([60]). De kan også videreformidle personopplysninger til en utenlandsk regjering eller internasjonal organisasjon for å oppfylle en rettslig forpliktelse i henhold til en traktat eller internasjonal konvensjon, i så fall skal de også oppfylle kravene som gjelder for overføring av opplysninger over landegrensene (se betraktning 90).

41) Prinsippene om lovlig og rettferdig behandling er derfor gjennomført i den sørkoreanske rettslige rammen på en måte som i det vesentlige svarer til forordning (EU) 2016/679, ved at behandling bare tillates av berettigede og klart definerte grunner. I alle nevnte tilfeller er behandlingen dessuten bare tillatt dersom det ikke er sannsynlig at den vil «krenke den registrertes eller en tredjeparts interesser urettmessig», noe som krever en avveining av interesser. I tillegg er det i artikkel 18 nr. 5 i PIPA fastsatt ytterligere garantier for når den behandlingsansvarlige videreformidler personopplysninger til en tredjepart, som kan omfatte en anmodning om å begrense formålet med og metoden for bruk eller om å innføre spesifikke sikkerhetstiltak. Tredjeparten plikter å gjennomføre tiltakene det anmodes om.

([56]) Overtredelser av artikkel 17 nr. 1 pkt. 1 i PIPA kan føre til strafferettslige sanksjoner (artikkel 71 nr. 1 i PIPA).

([57]) Det «tiltenkte formålet» er formålet som opplysningene ble samlet inn for. Dersom opplysningene for eksempel samles inn på grunnlag av den aktuelle personens samtykke, er det tiltenkte formålet det formålet som personen informeres om i henhold til artikkel 15 nr. 2 i PIPA.

([58]) Jf. artikkel 18 nr. 1 i PIPA. Overtredelser av artikkel 18 nr. 1 og 2 kan føre til strafferettslige sanksjoner (artikkel 71 nr. 2 i PIPA).

([59]) Leverandører av informasjons- og kommunikasjonstjenester kan bare bruke personopplysninger eller utlevere dem til en tredjepart for et annet formål enn det opprinnelige av grunnene angitt i artikkel 18 nr. 2 pkt. 1 og 2 i PIPA (det vil si dersom det er innhentet ytterligere samtykke, eller dersom det i lovgivningen er fastsatt særlige bestemmelser). Se artikkel 18 nr. 2 i PIPA.

([60]) Med mindre behandlingen er nødvendig for å etterforske og rettsforfølge straffbare forhold eller for å reise tiltale, skal offentlige institusjoner som bruker personopplysninger eller utleverer dem til en tredjepart for et annet formål enn formålet med innsamlingen (for eksempel dersom dette spesifikt er tillatt ved lov eller er nødvendig for å gjennomføre en traktat), offentliggjøre det rettslige grunnlaget for behandlingen og formålet med og omfanget av den på sitt nettsted eller i det offisielle kunngjøringsbladet og føre registre (artikkel 18 nr. 4 i PIPA og artikkel 15 i gjennomføringsdekretet til PIPA).

42) Artikkel 28-2 i PIPA gir mulighet for (videre) behandling av pseudonymiserte opplysninger uten den berørte personens samtykke for statistiske formål og formål knyttet til vitenskapelig forskning([61]) og arkivering i allmennhetens interesse, med forbehold for spesifikke garantier. I likhet med forordning (EU) 2016/679([62]) letter PIPA derfor (videre) behandling av personopplysninger for slike formål innenfor en ramme som gir egnede garantier for vern av enkeltpersoners rettigheter. I stedet for å bruke pseudonymisering som en mulig garanti er dette i PIPA fastsatt som en forutsetning for å utføre visse behandlingsaktiviteter for statistiske formål og formål knyttet til vitenskapelig forskning og arkivering i allmennhetens interesse (for eksempel for å kunne behandle opplysninger uten samtykke eller samkjøre forskjellige datasett).

43) PIPA inneholder i tillegg en rekke spesifikke garantier, særlig med hensyn til nødvendige tekniske og organisatoriske tiltak, registrering, begrensninger angående utveksling av opplysninger og håndtering av mulige farer for reidentifisering. Kombinasjonen av de forskjellige garantiene beskrevet i betraktning 44–48 sikrer at behandlingen av personopplysninger i denne sammenhengen i det vesentlige omfattes av det samme beskyttelsesnivået som det som kreves i forordning (EU) 2016/679.

44) For det første, og viktigst av alt, er det i henhold til artikkel 28-5 nr. 1 i PIPA forbudt å behandle pseudonymiserte opplysninger dersom formålet er å identifisere en bestemt person. Dersom det under behandlingen av pseudonymiserte opplysninger likevel genereres opplysninger som kan identifisere en person, må den behandlingsansvarlige umiddelbart avbryte behandlingen og tilintetgjøre slike opplysninger (artikkel 28-5 nr. 2 i PIPA). Manglende overholdelse av disse bestemmelsene straffes med overtredelsesgebyrer og utgjør et straffbart forhold([63]). Dette betyr at selv i situasjoner der det vil være *praktisk* mulig å reidentifisere personen, er slik reidentifisering *rettslig* forbudt.

45) For det andre skal den behandlingsansvarlige i forbindelse med (videre) behandling av pseudonymiserte opplysninger for slike formål treffe spesifikke teknologiske, organisatoriske og fysiske tiltak for å sikre opplysningenes sikkerhet (herunder separat lagring og forvaltning av de opplysningene som er nødvendige for å gjenopprette de pseudonymiserte opplysningenes opprinnelig form)([64]). Det må dessuten føres et register over de pseudonymiserte opplysningene som behandles, formålet med behandlingen, brukshistorikken og eventuelle tredjepartsmottakere (artikkel 29-5 nr. 2 i gjennomføringsdekretet til PIPA).

46) For det tredje inneholder PIPA spesifikke garantier for å hindre at tredjeparter kan identifisere enkeltpersoner dersom opplysningene utveksles. Behandlingsansvarlige som videreformidler pseudonymiserte opplysninger til en tredjepart for statistiske formål eller formål knyttet til vitenskapelig forskning eller arkivering i allmennhetens interesse, kan ikke ta med opplysninger som kan brukes til å identifisere en bestemt person (artikkel 28-2 nr. 2 i PIPA)([65]).

47) Mer spesifikt gir PIPA mulighet til å samkjøre pseudonymiserte opplysninger (behandlet av forskjellige behandlingsansvarlige) for statistiske formål eller formål knyttet til vitenskapelig forskning eller arkivering i allmennhetens interesse, men dette forbeholdes spesialiserte institusjoner utstyrt med spesifikke sikkerhetsfasiliteter (artikkel 28-3 nr. 1 i PIPA)([66]). Når en behandlingsansvarlig søker om å samkjøre pseudonymiserte opplysninger, må vedkommende sende

([61]) Vitenskapelig forskning defineres i artikkel 2 nr. 8 i PIPA som «forskning der det brukes vitenskapelige metoder, for eksempel teknologisk utvikling og demonstrasjon, grunnforskning, anvendt forskning og privatfinansiert forskning». Disse kategoriene svarer til kategoriene angitt i betraktning 159 i forordning (EU) 2016/679.

([62]) Se artikkel 5 nr. 1 bokstav b) og artikkel 89 nr. 1–2 samt betraktning 50 og 157 i forordning (EU) 2016/679.

([63]) Se artikkel 28-6 nr. 1, artikkel 71 nr. 4–3 og artikkel 75 nr. 2 pkt. 4–4 i PIPA.

([64]) Artikkel 28-4 i PIPA og artikkel 29-5 i gjennomføringsdekretet til PIPA. Manglende oppfyllelse av denne forpliktelsen er underlagt administrative og strafferettslige sanksjoner, se artikkel 73 nr. 1 og artikkel 75 nr. 2 pkt. 6 i PIPA.

([65]) Overtredelse av disse kravene kan føre til strafferettslige sanksjoner (artikkel 71 nr. 2 i PIPA). PIPC begynte å håndheve disse reglene med det samme, for eksempel i sin avgjørelse av 28. april 2021 der en bot og korrigerende tiltak ble ilagt et selskap som i tillegg til andre overtredelser av PIPA ikke oppfylte kravet i artikkel 28-2 nr. 2 i PIPA, se https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) For å bli utpekt som en slik spesialisert institusjon (et «ekspertorgan for samkjøring av opplysninger») må det inngis en søknad til PIPC sammen med underlagsdokumenter som blant annet må inneholde informasjon om fasilitetene og utstyret som finnes for å samkjøre pseudonymiserte opplysninger på en sikker måte, og som bekrefter at søkeren har minst tre fulltidsansatte med kvalifikasjoner eller erfaring innen vern av personopplysninger (artikkel 29-2 nr. 1 og 2 i gjennomføringsdekretet til PIPA). Detaljerte krav, for eksempel med hensyn til personalets kvalifikasjoner, tilgjengelige fasiliteter, sikkerhetstiltak og interne retningslinjer og prosedyrer, og finansielle krav er fastsatt i PIPCs melding 2020-9 om samkjøring og utlevering av pseudonymiserte opplysninger (plan I). PIPC kan tilbakekalle en utpeking som ekspertorgan for samkjøring av opplysninger (etter at det er avholdt samråd) av visse grunner, for eksempel dersom organet ikke lenger oppfyller sikkerhetsstandardene som kreves for utpekingen, eller dersom det har oppstått et brudd på opplysningssikkerheten i forbindelse med en samkjøring av opplysninger (artikkel 29-2 nr. 5 og 6 i gjennomføringsdekretet til PIPA). PIPC må offentliggjøre hver utpeking (eller tilbakekalling av en utpeking) av et ekspertorgan for samkjøring av opplysninger (artikkel 29-2 nr. 7 i gjennomføringsdekretet til PIPA).

inn dokumentasjon om blant annet opplysningene som skal samkjøres, formålet med samkjøringen og om de foreslåtte sikkerhetstiltakene for behandlingen av de samkjørte opplysningene([67]). For å kunne utføre samkjøringen må den behandlingsansvarlige sende opplysningene som skal samkjøres, til den spesialiserte institusjonen og stille til rådighet en «samkjøringsnøkkel» (det vil si opplysningene som er blitt brukt til pseudonymisering) for Republikken Koreas byrå for internett og sikkerhet([68]). Byrået genererer «data for lenking av samkjøringsnøkler» (som gjør det mulig å koble sammen samkjøringsnøkler fra forskjellige søkere for å samkjøre datasettene) og videreformidler dem til den spesialiserte institusjonen([69]).

48) Den behandlingsansvarlige som har anmodet om samkjøring, kan analysere de samkjørte opplysningene hos den spesialiserte institusjonen på et sted der det er innført spesifikke tekniske, fysiske eller administrative sikkerhetstiltak (artikkel 29-3 i gjennomføringsdekretet til PIPA). Behandlingsansvarlige som bidrar med et datasett til en slik samkjøring, kan bare eksportere de samkjørte opplysningene utenfor den spesialiserte institusjonen etter ytterligere pseudonymisering eller anonymisering av de samkjørte opplysningene og med den aktuelle institusjonens godkjenning (artikkel 28-3 nr. 2 i PIPA)([70]). Når institusjonen vurderer om det skal gis en slik godkjenning, skal den vurdere forholdet mellom de samkjørte opplysningene og formålet med behandlingen og om det er utarbeidet en spesifikk sikkerhetsplan for bruken av slike opplysninger([71]). Det er ikke tillatt å eksportere de samkjørte opplysningene utenfor institusjonen dersom de inneholder opplysninger som gjør det mulig å identifisere en person([72]). Den spesialiserte institusjonens samkjøring og utlevering av pseudonymiserte opplysninger overvåkes av PIPC (artikkel 29-4 nr. 3 i gjennomføringsdekretet til PIPA).

2.3.2 *Behandling av særlige kategorier av personopplysninger*

49) Det bør foreligge spesifikke garantier ved behandling av «særlige kategorier» av opplysninger.

50) PIPA inneholder særlige regler for behandling av sensitive opplysninger([73]), som defineres som personopplysninger som avdekker informasjon om en persons ideologi, tro, medlemskap eller avsluttet medlemskap i en fagforening eller et politisk parti, politiske oppfatning, helse og seksualliv samt andre personopplysninger som i «betydelig» grad kan true den registrertes personvern, og som ved presidentdekret er identifisert som sensitive opplysninger([74]). I henhold til presiseringene fra PIPC fortolkes seksualliv som at det også omfatter personens seksuelle legning eller preferanser([75]). Videre tilføyer artikkel 18 i gjennomføringsdekretet ytterligere kategorier til gruppen av sensitive opplysninger, særlig DNA-opplysninger fra genetisk testing og opplysninger fra en persons strafferegister. Den nylige endringen av gjennomføringsdekretet til PIPA har utvidet begrepet sensitive opplysninger ytterligere ved også å inkludere person-opplysninger som avdekker rase eller etnisk opprinnelse samt biometriske opplysninger([76]). Etter denne endringen tilsvarer begrepet sensitive opplysninger i PIPA i det vesentlige det som er angitt i artikkel 9 i forordning (EU) 2016/679.

51) I henhold til artikkel 23 nr. 1 i PIPA og i likhet med det som er fastsatt i artikkel 9 nr. 1 i forordning (EU) 2016/679, er behandling av sensitive opplysninger generelt sett forbudt, med mindre et av de nevnte unntakene får anvendelse([77]). Disse begrenser behandlingen til tilfeller der den behandlingsansvarlige underretter den registrerte i samsvar med

([67]) Artikkel 8 nr. 1 og 2 i melding 2020-9 om samkjøring og utlevering av pseudonymiserte opplysninger.
([68]) Artikkel 2 nr. 3 og 6 og artikkel 9 nr. 1 i melding 2020-9 om samkjøring og utlevering av pseudonymiserte opplysninger.
([69]) Artikkel 2 nr. 4 og artikkel 9 nr. 2 og 3 i melding 2020-9 om samkjøring og utlevering av pseudonymiserte opplysninger. Den spesialiserte institusjonen må umiddelbart tilintetgjøre opplysningene for lenking av samkjøringsnøkler etter en samkjøring (artikkel 9 nr. 4 i meldingen).
([70]) Overtredelse av kravene som gjelder samkjøring av datasett, kan føre til strafferettslige sanksjoner (artikkel 71 nr. 4-2 i PIPA). Se også artikkel 29-2 nr. 4 i gjennomføringsdekretet til PIPA.
([71]) Framgangsmåten for å godkjenne en utlevering av samkjørte opplysninger er fastsatt i artikkel 11 i melding 2020-9 om samkjøring og utlevering av pseudonymiserte opplysninger. Den spesialiserte institusjonen må særlig nedsette et «utvalg for gjennomgåelse av utleveringen» bestående av medlemmer med inngående kjennskap til og erfaring med vern av opplysninger.
([72]) Artikkel 29-2 nr. 4 i gjennomføringsdekretet til PIPA og melding 2020-9 artikkel 11.
([73]) Den sørkoreanske forfatningsdomstolen har også erkjent behovet for et spesifikt vern i forbindelse med behandling av sensitive opplysninger, for eksempel opplysninger som gjelder helse eller seksuell atferd, se forfatningsdomstolens avgjørelse HunMa 1139 av 31. mai 2007.
([74]) Artikkel 23 nr. 1 i PIPA.
([75]) Se også kapittel III avsnitt 2 om artikkel 23 (s. 157–164) i håndboken for PIPA.
([76]) Det vil si personopplysninger som følger av en spesifikk teknisk behandling av opplysninger om en persons fysiske, fysiologiske eller atferdsmessige egenskaper for det formålet å entydig identifisere vedkommende.
([77]) Manglende oppfyllelse av disse kravene kan føre til sanksjoner i henhold til artikkel 71 pkt. 3 i PIPA.

artikkel 15 og 17 i PIPA, og innhenter et separat samtykke (det vil si i tillegg til samtykket til behandling av andre personopplysninger), eller dersom behandlingen er påkrevd eller tillatt ved lov. Offentlige myndigheter kan også behandle biometriske opplysninger, DNA-opplysninger oppnådd ved genetisk testing, personopplysninger som avdekker rase eller etnisk opprinnelse, og opplysninger fra et strafferegister av grunner som bare de kan påberope seg (for eksempel dersom det er nødvendig for å etterforske straffbare forhold eller for at en domstol skal kunne behandle en sak)([78]). Det rettslige grunnlaget for behandling av sensitive opplysninger er mer begrenset enn for andre typer personopplysninger, og enda mer restriktivt i sørkoreansk rett enn det er i artikkel 9 nr. 2 i forordning (EU) 2016/679.

52) I artikkel 23 nr. 2 i PIPA – manglende overholdelse av denne kan medføre sanksjoner([79]) – understrekes det dessuten at det er spesielt viktig å sørge for tilstrekkelig sikkerhet ved håndtering av sensitive opplysninger, slik at de ikke «kan gå tapt, stjeles, gis videre, forfalskes, endres eller skades». Selv om dette er et generelt krav i henhold til artikkel 29 i PIPA, gjør artikkel 3 nr. 4 det klart at sikkerhetsnivået må tilpasses den typen personopplysninger som behandles, noe som betyr at det må tas hensyn til de særlige risikoene som er forbundet med behandling av sensitive opplysninger. Behandlingen av opplysningene skal dessuten alltid utføres «på en måte som minimerer muligheten for å krenke» den registrertes personvern, og om mulig «anonymt» (artikkel 3 nr. 6 og 7 i PIPA). Disse kravene er særlig relevante når behandlingen gjelder sensitive opplysninger.

2.3.3 *Formålsbegrensning*

53) Personopplysninger bør samles inn for et spesifikt formål og på en måte som er forenlig med formålet med behandlingen.

54) Dette prinsippet sikres ved artikkel 3 nr. 1 og 2 i PIPA, der det er fastsatt at den behandlingsansvarlige skal «spesifisere og uttrykkelig angi» formålet med behandlingen og behandle personopplysninger på en måte som er egnet og nødvendig for nevnte formål, og ikke bruke dem for andre formål. Det generelle prinsippet om formålsbegrensning bekreftes også i artikkel 15 nr. 1, artikkel 18 nr. 1, artikkel 19 og – for databehandlere (såkalte «underleverandører») – i artikkel 26 nr. 1 pkt. 1 og artikkel 26 nr. 5 og 7 i PIPA. Personopplysninger kan i prinsippet bare brukes og videreformidles til tredjeparter innenfor rammen av formålet som de ble innsamlet for (artikkel 15 nr. 1 og artikkel 17 nr. 1 pkt. 2). Behandling for et forenlig formål, det vil si «innenfor rammer som er rimelig knyttet til det opprinnelige formålet med innsamlingen», må bare finne sted dersom det ikke påvirker de berørte registrerte negativt, og dersom det treffes nødvendige sikkerhetstiltak (for eksempel kryptering) (artikkel 15 nr. 3 og artikkel 17 nr. 4 i PIPA). For å avgjøre om videre behandling er for et forenlig formål, inneholder gjennomføringsdekretet til PIPA spesifikke kriterier som svarer til de som er fastsatt i artikkel 6 nr. 4 i forordning (EU) 2016/679, se betraktning 36.

55) Som forklart i betraktning 38 er formålet med innsamlingen når det gjelder sørkoreanske behandlingsansvarlige som mottar personopplysninger fra Unionen, det formålet som opplysningene overføres for. Den behandlingsansvarlige kan bare unntaksvis og i spesifikke (angitte) tilfeller endre formålet (artikkel 18 nr. 2 pkt. 1–3 i PIPA, se også betraktning 39). Dersom en endring av formålet er tillatt ved lov, skal slike lover respektere den grunnleggende retten til personvern og vern av personopplysninger samt prinsippene om nødvendighet og forholdsmessighet fastsatt i den sørkoreanske forfatningen. Artikkel 18 nr. 2 og 5 i PIPA inneholder dessuten ytterligere garantier, særlig kravet om at en slik formålsendring ikke må «krenke den registrertes interesser urettmessig», noe som alltid krever en avveining av interesser. Dette sikrer et beskyttelsesnivå som i det vesentlige tilsvarer det som er angitt i artikkel 5 nr. 1 bokstav b) og artikkel 6 sammenholdt med betraktning 50 i forordning (EU) 2016/679.

2.3.4 *Opplysningenes riktighet og dataminimering*

56) Personopplysninger skal være riktige og, når det er nødvendig, oppdaterte. De skal også være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for.

([78]) I henhold til artikkel 18 i gjennomføringsdekretet til PIPA er kategoriene av opplysninger angitt der unntatt fra bestemmelsen i lovens artikkel 23 nr. 1 når de behandles av en offentlig institusjon i henhold til artikkel 18 nr. 2 pkt. 5–9 i PIPA.

([79]) Se artikkel 73 nr. 1 og artikkel 75 nr. 2 pkt. 6 i PIPA.

57) Prinsippet om riktighet anerkjennes i artikkel 3 nr. 3 i PIPA, der det kreves at personopplysninger skal være «riktige, fullstendige og oppdaterte i det omfang som er nødvendig for formålene» som opplysningene behandles for. Dataminimering kreves i henhold til artikkel 3 nr. 1 og 6 og artikkel 16 nr. 1 i PIPA, der det er angitt at den behandlingsansvarlige skal samle inn personopplysninger (bare) «i så lite omfang som nødvendig» for det tiltenkte formålet, og at vedkommende har bevisbyrden med hensyn til dette. Dersom det er mulig å oppfylle formålet med innsamlingen ved å behandle opplysningene i anonymisert form, bør de behandlingsansvarlige bestrebe seg på å gjøre dette (artikkel 3 nr. 7 i PIPA).

2.5.3 *Lagringsbegrensning*

58) Personopplysninger bør i prinsippet ikke lagres lenger enn det som er nødvendig for formålene som personopplysningene behandles for.

59) Prinsippet om lagringsbegrensning er fastsatt i artikkel 21 nr. 1 i PIPA([80]), der det kreves at den behandlingsansvarlige uten opphold skal «tilintetgjøre»([81]) personopplysninger når formålet med behandlingen er oppnådd, eller når lagringstiden er utløpt (alt etter hva som inntreffer først), med mindre ytterligere lagring kreves ved lov([82]). I sistnevnte tilfelle skal de aktuelle personopplysningene «lagres og håndteres atskilt fra andre personopplysninger» (artikkel 21 nr. 3 i PIPA).

60) Artikkel 21 nr. 1 i PIPA får ikke anvendelse når pseudonymiserte opplysninger behandles for statistiske formål eller formål knyttet til vitenskapelig forskning eller arkivering i allmennhetens interesse([83]). For å sikre prinsippet om begrenset lagring av opplysninger også i slike tilfeller kreves det i henhold til melding 2021-5 at behandlingsansvarlige skal anonymisere opplysningene i samsvar med artikkel 58-2 i PIPA dersom opplysningene ikke er blitt tilintetgjort når det spesifikke formålet med behandlingen er oppnådd([84]).

2.3.6 *Personopplysningssikkerhet*

61) Personopplysninger bør behandles på en måte som gjør at sikkerheten garanteres, herunder at opplysningene vernes mot uautorisert eller ulovlig behandling og mot utilsiktet tap, tilintetgjøring eller skade. For dette formålet bør økonomiske operatører treffe egnede tekniske eller organisatoriske tiltak for å verne personopplysninger mot mulige trusler. Ved vurderingen av disse tiltakene bør det tas hensyn til den teknologiske utviklingen, kostnadene og behandlingens art, omfang, sammenheng og formål samt risikoene for den enkeltes rettigheter.

62) Et lignende sikkerhetsprinsipp er fastsatt i artikkel 3 nr. 4 i PIPA, der det kreves at behandlingsansvarlige skal «håndtere personopplysninger på en sikker måte i henhold til behandlingsmetodene for og typene osv. av personopplysninger, idet det tas hensyn til risikoen for å krenke den registrertes rettigheter og hvor alvorlige de aktuelle risikoene er». Den behandlingsansvarlige skal dessuten «behandle personopplysninger på en måte som gjør at risikoen for å krenke en registrerts personvern minimeres», og skal i denne forbindelse bestrebe seg på å behandle personopplysninger anonymt eller i pseudonymisert form dersom det er mulig (artikkel 3 nr. 6 og 7 i PIPA).

63) Disse generelle kravene utdypes ytterligere i artikkel 29 i PIPA, der det er angitt at hver behandlingsansvarlig «skal treffe de tekniske, organisatoriske og fysiske tiltakene, for eksempel utarbeide en intern styringsplan og oppbevare innloggingsregistre osv., som er nødvendige for å garantere sikkerheten som angitt ved presidentdekret, slik at

([80]) Artikkel 8 (sammenholdt med artikkel 8-2 i gjennomføringsdekretet), artikkel 11 (sammenholdt med artikkel 12 nr. 2 i gjennomføringsdekretet).

([81]) Når det gjelder metodene for tilintetgjøring av personopplysninger, vises det til artikkel 16 i gjennomføringsdekretet til PIPA. I artikkel 21 nr. 2 i PIPA presiseres det at dette skal omfatte «nødvendige tiltak for å hindre gjenfinning eller gjenoppretting».

([82]) Dersom disse kravene ikke oppfylles, kan det føre til strafferettslige sanksjoner (artikkel 73 nr. 1 og 2 i PIPA). Ved artikkel 39-6 i PIPA pålegges leverandører av informasjons- og kommunikasjonstjenester et ytterligere krav om å slette personopplysninger om brukere som ikke har gjort bruk av de tilbudte informasjons- og kommunikasjonstjenestene i løpet av minst et år (med mindre ytterligere lagring kreves ved lov eller brukeren ber om det). Enkeltpersoner må informeres om den planlagte slettingen av deres opplysninger 30 dager før utløpet av fristen på et år (artikkel 39-6 nr. 2 i PIPA og artikkel 48-5 nr. 3 i gjennomføringsdekretet til PIPA). Dersom loven krever ytterligere lagring, må de lagrede opplysningene lagres atskilt fra andre opplysninger om brukere og kan bare brukes eller utleveres i samsvar med den aktuelle loven (artikkel 48-5 nr. 1 og 2 i gjennomføringsdekretet til PIPA).

([83]) Artikkel 28-7 i PIPA.

([84]) Melding 2021-5 avsnitt 4 (vedlegg I).

personopplysningene ikke går tapt, stjeles, videreformidles, forfalskes, endres eller skades». Disse tiltakene presiseres i artikkel 30 nr. 1 i gjennomføringsdekretet til PIPA, der det vises til 1) utarbeidingen og gjennomføringen av en intern styringsplan for sikker behandling av personopplysninger, 2) tilgangskontroll og -begrensninger, 3) innføring av krypteringsteknologi for sikker lagring og overføring av personopplysninger, 4) innloggingsregistre, 5) sikkerhetsprogrammer og 6) fysiske tiltak, for eksempel et sikkert lagrings- eller låsesystem([85]).

64) Ved brudd på opplysningssikkerheten gjelder det i tillegg særlige forpliktelser (artikkel 34 i PIPA sammenholdt med artikkel 39 og 40 i gjennomføringsdekretet til PIPA)([86]). Den behandlingsansvarlige plikter særlig å uten opphold gi de berørte registrerte mer detaljert informasjon om bruddet([87]), herunder informasjon om mottiltak (tvangstiltak) som den behandlingsansvarlige har truffet, og om hva de registrerte kan gjøre for å minimere risikoen for skade (artikkel 34 nr. 1 og 2 i PIPA)([88]). Dersom bruddet på opplysningssikkerheten gjelder minst 1 000 registrerte, skal den behandlingsansvarlige uten opphold også rapportere bruddet og mottiltakene som er truffet, til PIPC og Republikken Koreas byrå for internett og sikkerhet, som kan yte teknisk bistand (artikkel 34 nr. 3 i PIPA sammenholdt med artikkel 39 i gjennomføringsdekretet til PIPA). Behandlingsansvarlige er ansvarlige for skader som følge av brudd på opplysningssikkerheten i samsvar med sivillovens bestemmelser om ansvar utenfor kontraktsforhold (se også avsnitt 2.5 om prøvings- og klageadgang)([89]).

65) For å oppfylle sine sikkerhetsforpliktelser må den behandlingsansvarlige bistås av en personvernansvarlig som blant annet skal ha som oppgave å utarbeide et internt kontrollsystem «for å hindre videreformidling, misbruk og feil bruk av personopplysninger» (artikkel 31 nr. 2 pkt. 4 i PIPA). Den behandlingsansvarlige plikter også å gjennomføre «egnet kontroll og overvåking» av personalet som behandler personopplysninger, herunder med henblikk på sikker håndtering. Dette omfatter nødvendig opplæring («utdanning») av ansatte (artikkel 28 nr. 1 og 2 i PIPA). Ved utkontraktert behandling må den behandlingsansvarlige også stille krav til «underleverandøren», blant annet med henblikk på sikker håndtering av personopplysninger («tekniske og organisatoriske garantier»), og må ved hjelp av inspeksjoner overvåke hvordan disse gjennomføres (artikkel 26 nr. 1 og 4 i PIPA sammenholdt med artikkel 28 nr. 1 pkt. 3, 4 og 6 i gjennomføringsdekretet til PIPA).

2.3.7 *Åpenhet*

66) De registrerte bør informeres om hovedtrekkene i behandlingen av deres personopplysninger.

([85]) Når det gjelder leverandører av informasjons- og kommunikasjonstjenesters behandling av personopplysninger, er det i artikkel 39-5 i PIPA uttrykkelig fastsatt at antall personer som håndterer personopplysninger om brukere, skal begrenses til et minimum. Leverandører av informasjons- og kommunikasjonstjenester skal dessuten sikre at brukernes personopplysninger ikke eksponeres for offentligheten via informasjons- og kommunikasjonsnettverket (artikkel 39-10 nr. 1 i PIPA). Eksponerte opplysninger må slettes eller blokkeres på anmodning fra PIPC (artikkel 39-10 nr. 2 i PIPA). Mer generelt er leverandører av informasjons- og kommunikasjonstjenester (og tredjeparter som mottar brukernes personopplysninger) underlagt ytterligere sikkerhetsforpliktelser, som angis i artikkel 48-2 i gjennomføringsdekretet til PIPA, for eksempel utarbeiding og gjennomføring av en intern styringsplan for sikkerhetstiltak, tiltak for å sikre tilgangskontroll, kryptering, bruk av programvare for å oppdage skadelig programvare osv.

([86]) I tillegg er det et generelt forbud mot å skade, tilintetgjøre, endre, forfalske eller lekke personopplysninger uten rettslig myndighet, se artikkel 59 pkt. 3 i PIPA.

([87]) Kravet om underretning av personen får ikke anvendelse dersom det oppstår et brudd på opplysningssikkerheten i forbindelse med pseudonymiserte opplysninger som behandles for statistiske formål eller formål knyttet til vitenskapelig forskning eller arkivering i allmennhetens interesse (artikkel 28-7 i PIPA, som inneholder et unntak fra artikkel 34 nr. 1 og 39-4 i PIPA). Individuell underretning vil kreve at den berørte behandlingsansvarlige identifiserer personer ut fra det pseudonymiserte datasettet, noe som er uttrykkelig forbudt i henhold til artikkel 28-5 i PIPA. Det generelle kravet om å underrette PIPC om bruddet på opplysningssikkerheten gjelder imidlertid fortsatt.

([88]) Kravene som gjelder underretning, blant annet tidspunkt og muligheten for at underretningen kan skje «trinnvis», presiseres nærmere i artikkel 40 i gjennomføringsdekretet til PIPA. Det gjelder strengere regler for leverandører av informasjons- og kommunikasjonstjenester, som plikter å underrette den registrerte og PIPC senest 24 timer etter at de er blitt klar over at personopplysninger er gått tapt, stjålet eller lekket (artikkel 39-4 nr. 1 i PIPA). Denne underretningen må inneholde nærmere opplysninger om personopplysningene som er lekket, når dette skjedde, tiltakene som brukeren kan treffe, mottiltak som leverandøren har truffet, og kontaktopplysningene til avdelingen som brukeren kan stille spørsmål til (artikkel 39-4 nr. 1 pkt. 1–5 i PIPA). Dersom det er en rimelig grunn, for eksempel at brukerens kontaktopplysninger ikke foreligger, kan underretningen skje på andre måter, for eksempel ved å gjøre informasjonen offentlig tilgjengelig på et nettsted (artikkel 39-4 nr. 1 i PIPA sammenholdt med artikkel 48-4 nr. 4 ff. i gjennomføringsdekretet til PIPA). I slike tilfeller må PIPC informeres om grunnene (artikkel 34-4 nr. 3 i PIPA).

([89]) Se for eksempel høyesteretts avgjørelse 2011Da59834, 2011Da59858 og 2011Da59841 av 26. desember 2012. Et sammendrag på engelsk er tilgjengelig på http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

67) Dette sikres på forskjellige måter i det sørkoreanske systemet. Foruten retten til informasjon i henhold til artikkel 4 pkt. 1 (generelt) og artikkel 20 nr. 1 i PIPA (for personopplysninger samlet inn fra tredjeparter) samt retten til innsyn i henhold til artikkel 35 i PIPA inneholder PIPA et generelt krav om åpenhet når det gjelder formålet med behandlingen (artikkel 3 nr. 1 i PIPA), og spesifikke krav om åpenhet dersom behandlingen er basert på samtykke (artikkel 15 nr. 2, artikkel 17 nr. 2 og artikkel 18 nr. 3 i PIPA)([90]). Ved artikkel 20 nr. 2 i PIPA kreves det også at visse behandlingsansvarlige – de der behandlingen overskrider visse terskler([91]) – skal underrette den registrerte som de har mottatt personopplysninger om fra en tredjepart, om kilden til opplysningene, formålet med behandlingen og den registrertes rett til å kreve at behandlingen innstilles, med mindre en slik underretning viser seg å være umulig på grunn av manglende kontaktopplysninger. Det gjelder unntak for visse personopplysningsfiler som innehas av myndighetene, særlig filer som inneholder opplysninger som behandles for formål knyttet til nasjonal sikkerhet, andre spesielt viktige («alvorlige») nasjonale interesser eller formål knyttet til strafferettslig håndheving, eller dersom det er sannsynlig at underretningen vil skade en annen persons liv eller legeme, eller urettmessig vil skade en annen persons eiendom eller andre interesser, men bare dersom de aktuelle offentlige eller private interessene «klart går foran» den berørte registrertes rettigheter (artikkel 20 nr. 4 i PIPA). Dette krever en avveining av interesser.

68) I artikkel 3 nr. 5 i PIPA er det også fastsatt at behandlingsansvarlige skal offentliggjøre sitt personvernprogram (og andre elementer knyttet til behandling av personopplysninger). Dette kravet presiseres ytterligere i artikkel 30 i PIPA sammenholdt med artikkel 31 i gjennomføringsdekretet til PIPA. I henhold til disse bestemmelsene må personvernprogrammet som offentliggjøres, blant annet inneholde informasjon om 1) hvilke typer personopplysninger som behandles, 2) formålet med behandlingen, 3) hvor lenge opplysningene vil bli lagret, 4) om personopplysningene vil bli utlevert til en tredjepart([92]), 5) enhver form for utkontraktert behandling, 6) den registrertes rettigheter og hvordan disse kan utøves, og 7) kontaktopplysninger (herunder navnet på den personvernansvarlige eller den interne avdelingen med ansvar for klagebehandling og for å sikre at reglene for vern av personopplysninger overholdes). Personvernprogrammet må offentliggjøres på måte som gjør at de registrerte «lett kan gjenkjenne det» (artikkel 30 nr. 2 i PIPA)([93]), og må oppdateres løpende (artikkel 31 nr. 2 i gjennomføringsdekretet til PIPA).

69) Offentlige institusjoner omfattes av en ytterligere forpliktelse til å registrere opplysninger hos PIPC, særlig følgende: 1) Den offentlige institusjonens navn, 2) grunnene til og formålene med behandlingen av personopplysningsfilene, 3) nærmere opplysninger om personopplysningene som registreres, 4) behandlingsmetoden, 5) hvor lenge opplysningene vil bli lagret, 6) antall registrerte som det lagres personopplysninger om, 7) avdelingen som håndterer anmodninger fra registrerte, og 8) mottakerne av personopplysninger dersom opplysningene videreformidles rutinemessig eller gjentatte ganger (artikkel 32 nr. 1 i PIPA)([94]). Registrerte personopplysningsfiler offentliggjøres av PIPC, og offentlige institusjoner må også vise til dem i sitt personvernprogram (artikkel 30 nr. 1 og artikkel 32 nr. 4 i PIPA).

70) For å øke åpenheten for registrerte i Unionen som får sine personopplysninger overført til Republikken Korea på grunnlag av denne beslutningen, er det innført ytterligere krav til åpenhet i avsnitt 3 punkt i) og ii) i melding 2021-5 (vedlegg I). For det første må sørkoreanske behandlingsansvarlige som mottar personopplysninger fra Unionen på grunnlag av denne beslutningen, uten unødig opphold (og ikke under noen omstendigheter senere enn én måned etter overføringen) underrette de berørte registrerte om navnet på og kontaktopplysningene til enhetene som overfører og

([90]) Når personopplysninger behandles med en persons samtykke, må den behandlingsansvarlige særlig informere vedkommende om formålet med behandlingen, hvilke opplysninger som vil bli behandlet, mottakeren av opplysningene, hvor lenge personopplysningene vil bli lagret og brukt, og om at personen har rett til å nekte å gi samtykke (og eventuelle ulemper som dette vil medføre).

([91]) I henhold til artikkel 15-2 nr. 1 i gjennomføringsdekretet til PIPA gjelder dette behandlingsansvarlige som behandler sensitive opplysninger om minst 50 000 registrerte, eller «normale» personopplysninger om minst 1 million registrerte. I artikkel 15-2 nr. 2 i gjennomføringsdekretet til PIPA angis metodene for underretningen og tidspunktene for når den skal skje, og i artikkel 15-2 nr. 3 angis kravet om å føre visse registre over dette. I tillegg gjelder det særlige regler for visse kategorier av leverandører av informasjons- og kommunikasjonstjenester (leverandører med salgsinntekter på minst KRW 10 milliarder i det foregående året, eller leverandører som lagrer/håndterer personopplysninger for minst én million brukere per dag i gjennomsnitt i de tre månedene før utgangen av det foregående året), som plikter å underrette brukerne regelmessig om hvordan deres personopplysninger er blitt brukt, med mindre dette viser seg å være umulig på grunn av manglende kontaktopplysninger (artikkel 39-8 i PIPA og artikkel 48-6 i gjennomføringsdekretet til PIPA).

([92]) I henhold til informasjonen som den sørkoreanske regjeringen har framlagt, innebærer dette en forpliktelse til å angi mottakeren/mottakerne individuelt i det offentlige personvernprogrammet.

([93]) Det er fastsatt ytterligere bestemmelser i artikkel 31 nr. 3 i gjennomføringsdekretet til PIPA.

([94]) Registreringskravet gjelder ikke for visse typer av personopplysningsfiler, for eksempel slike der det registreres opplysninger knyttet til nasjonal sikkerhet, diplomatiske hemmeligheter, strafferettslig etterforskning, rettsforfølgning, straff, etterforskning av skatterelaterte straffbare forhold, eller som utelukkende gjelder interne arbeidsprestasjoner (artikkel 32 nr. 2 i PIPA).

mottar opplysningene, personopplysningene (eller kategorien av personopplysninger) som er overført, den sørkoreanske behandlingsansvarliges formål med innsamlingen, hvor lenge opplysningene lagres, og rettighetene i henhold til PIPA. For det andre må de registrerte, når personopplysninger som er mottatt fra Unionen på grunnlag av denne beslutningen, videreformidles til tredjeparter, blant annet informeres om mottakeren, personopplysningene eller kategoriene av personopplysningene som skal videreformidles, landet som opplysningene skal videreformidles til (dersom det er relevant), og rettighetene i henhold til PIPA([95]). På denne måten sikrer nevnte melding at enkeltpersoner i EU fortsatt informeres om de spesifikke behandlingsansvarlige som behandler deres opplysninger, og at de kan utøve sine rettigheter overfor de relevante enhetene.

71) I avsnitt 3 punkt iii) i meldingen (vedlegg I) tillates visse begrensede og kvalifiserte unntak fra disse ytterligere kravene til åpenhet som i det vesentlige tilsvarer de som er fastsatt i forordning (EU) 2016/679. Det kreves ikke at registrerte i Unionen underrettes 1) dersom og så lenge det er nødvendig å begrense underretningen av visse grunner knyttet til allmennhetens interesse (for eksempel når opplysningene behandles for formål knyttet til nasjonal sikkerhet eller en pågående strafferettslig etterforskning), i den grad disse målene i allmennhetens interesse klart går foran den registrertes rettigheter, 2) dersom den registrerte allerede har informasjonen, (3) dersom og så lenge det er sannsynlig at underretning vil skade personens eller en annen persons liv eller legeme eller urettmessig krenke en annen persons eiendomsinteresser, dersom disse rettighetene eller interessene klart går foran den registrertes rettigheter, eller 4) dersom det ikke finnes kontaktopplysninger for de berørte enkeltpersonene, eller dersom det kreves en uforholdsmessig stor innsats for å underrette dem. Ved vurderingen av om det er mulig å kontakte den registrerte, eller om dette innebærer en uforholdsmessig stor innsats, skal muligheten for å samarbeide med dataeksportøren i Unionen tas i betraktning.

72) Reglene i betraktning 67–71 sikrer derfor et beskyttelsesnivå som når det gjelder åpenhet, i det vesentlige tilsvarer det som er fastsatt i forordning (EU) 2016/679.

2.3.8 *Individuelle rettigheter*

73) Registrerte bør ha visse rettigheter som kan gjøres gjeldende overfor den behandlingsansvarlige eller databehandleren, særlig retten til innsyn i opplysninger, retten til å få opplysninger rettet, retten til å protestere mot behandlingen og retten til å få opplysninger slettet. Samtidig kan slike rettigheter være underlagt begrensninger i den grad disse begrensningene er nødvendige og forholdsmessige for å beskytte viktige mål av allmenn interesse.

74) I henhold til artikkel 3 nr. 5 i PIPA skal den behandlingsansvarlige garantere de registrertes rettigheter som angitt i artikkel 4 i PIPA og som ytterligere presisert i artikkel 35–37, artikkel 39 og artikkel 39-2 i PIPA.

75) For det første har enkeltpersoner rett til informasjon og innsyn. Når den behandlingsansvarlige har samlet inn personopplysninger fra en tredjepart – noe som alltid vil være tilfellet når opplysningene overføres fra Unionen – har de registrerte generelt sett rett til å få informasjon om 1) «kilden» til personopplysningene som er samlet inn (det vil si den overførende parten), 2) formålet med behandlingen og 3) at de har rett til å kreve at behandlingen innstilles (artikkel 20 nr. 1 i PIPA). Det gjelder begrensede unntak, særlig dersom det er sannsynlig at dette vil skade en annen persons liv eller legeme eller «urettmessig skade en annen persons eiendom og andre interesser», men bare dersom disse tredjepartenes interesser går «klart foran» den registrertes rettigheter (artikkel 20 nr. 4 pkt. 2 i PIPA).

76) Ved artikkel 35 nr. 1 og 3 i PIPA sammenholdt med artikkel 41 nr. 4 i gjennomføringsdekretet til PIPA gis de registrerte dessuten rett til innsyn i egne personopplysninger([96]). Retten til innsyn omfatter en bekreftelse på behandlingen, informasjon om hvilken type opplysninger som behandles, formålet med behandlingen, hvor lenge opplysningene vil bli lagret, og en eventuell utlevering til en tredjepart samt utlevering av en kopi av personopplysningene som er behandlet

([95]) Melding 2021-5 avsnitt 3 punkt ii) (vedlegg I).

([96]) I henhold til artikkel 35 nr. 3 i PIPA sammenholdt med artikkel 42 nr. 2 i gjennomføringsdekretet til PIPA kan den behandlingsansvarlige utsette innsynet dersom det er «en god grunn» til det (det vil si berettigede grunner, for eksempel dersom det er behov for mer tid for å vurdere om det kan gis innsyn), men må underrette den registrerte om dette innen ti dager og opplyse om hvordan det kan klages på denne avgjørelsen. Så snart grunnene til utsettelsen ikke lenger foreligger, skal det gis innsyn.

(artikkel 4 pkt. 3 i PIPA sammenholdt med artikkel 41 nr. 1 i gjennomføringsdekretet til PIPA)([97]). Innsynet kan bare begrenses (delvis innsyn)([98]) eller nektes dersom dette er fastsatt ved lov([99]), dersom det er sannsynlig at det vil skade en tredjeparts liv eller legeme eller urettmessig krenke en annen persons eiendom og andre interesser (artikkel 35 nr. 4 i PIPA)([100]). Det sistnevnte innebærer at det skal foretas en avveining mellom den enkeltes og andre personers forfatningssikrede rettigheter og friheter. Dersom innsynet begrenses eller nektes, må den behandlingsansvarlige underrette den registrerte om grunnene til dette og om hvordan det kan klages på avgjørelsen (artikkel 41 nr. 5 og artikkel 42 nr. 2 i gjennomføringsdekretet til PIPA).

77) For det andre har registrerte rett til å få sine personopplysninger rettet eller slettet([101]), «med mindre annet er uttrykkelig fastsatt i andre lover» (artikkel 36 nr. 1 og 2 i PIPA)([102]). Etter å ha mottatt en anmodning må den behandlingsansvarlige uten opphold undersøke saken, treffe nødvendige tiltak([103]) og underrette den registrerte om dette innen ti dager. Dersom anmodningen ikke kan oppfylles, innebærer dette kravet om underretning at det skal opplyses om grunnene til avslaget, og om hvordan det kan klages på avgjørelsen (se artikkel 36 nr. 4 i PIPA sammenholdt med artikkel 43 nr. 3 i gjennomføringsdekretet til PIPA)([104]).

78) For det tredje har registrerte rett til å få innstilt behandlingen av sine personopplysninger uten opphold([105]), med mindre et av de angitte unntakene får anvendelse (artikkel 37 nr. 1 og 2 i PIPA)([106]). Den behandlingsansvarlige kan avslå dette 1) dersom dette er uttrykkelig tillatt ved lov eller er nødvendig («uunngåelig») for å oppfylle rettslige forpliktelser, 2) dersom det er sannsynlig at den innstilte behandlingen vil skade en tredjeparts liv eller legeme eller urettmessig krenke en annen persons eiendom og andre interesser, 3) dersom det ikke vil være mulig for en offentlig institusjon å utføre lovfestede oppgaver uten å behandle opplysningene, eller 4) dersom den registrerte ikke uttrykkelig sier opp den underliggende avtalen med den behandlingsansvarlige, selv om det ikke vil være praktisk mulig å gjennomføre avtalen uten slik behandling av opplysninger. Da må den behandlingsansvarlige uten opphold underrette den registrerte om grunnene til avslaget og om hvordan det kan klages på avgjørelsen (artikkel 37 nr. 2 i PIPA sammenholdt med artikkel 44 nr. 2 i gjennomføringsdekretet til PIPA). I henhold til artikkel 37 nr. 4 i PIPA må den behandlingsansvarlige uten opphold «treffe nødvendige tiltak, herunder tilintetgjøring av de relevante personopplysningene», for å oppfylle anmodningen om å få behandlingen innstilt([107]).

79) Retten til å få behandlingen innstilt gjelder også når personopplysninger brukes til direkte markedsføring, det vil si for å markedsføre varer eller tjenester eller oppfordre til kjøp av dem. En slik videre behandling krever dessuten generelt sett den registrertes spesifikke (nye) samtykke (se artikkel 15 nr. 1 pkt. 1 og artikkel 17 nr. 2 pkt. 1 i PIPA)([108]). Når den behandlingsansvarlige ber om dette samtykket, må den registrerte særlig informeres om den tiltenkte bruken av

([97]) Innsyn i personopplysninger som behandles av en offentlig institusjon, kan oppnås direkte fra institusjonen eller indirekte ved å inngi en anmodning til PIPC, som uten opphold skal videresende anmodningen (artikkel 35 nr. 2 i PIPA og artikkel 41 nr. 3 i gjennomførings-dekretet til PIPA).

([98]) I henhold til artikkel 42 nr. 1 i gjennomføringsdekretet til PIPA plikter den behandlingsansvarlige å gi delvis innsyn dersom minst en del av opplysningene ikke omfattes av begrunnelsen for avslaget.

([99]) Slike lover må respektere den grunnleggende retten til personvern og retten til vern av personopplysninger samt prinsippene om nødvendighet og forholdsmessighet fastsatt i den sørkoreanske forfatningen.

([100]) Offentlige institusjoner kan dessuten nekte å gi innsyn dersom det vil kunne forårsake alvorlige problemer med å gjennomføre visse oppgaver, herunder løpende revisjoner eller ilegging, inndriving eller tilbakebetaling av skatter (artikkel 35 nr. 4 i PIPA).

([101]) I dette tilfellet må den behandlingsansvarlige treffe tiltak for å hindre at personopplysningene gjenopprettes, se artikkel 36 nr. 3 i PIPA.

([102]) Slike lover må oppfylle kravene i forfatningen om at en grunnleggende rettighet bare kan begrenses når det er nødvendig av hensyn til den nasjonale sikkerheten eller for å opprettholde lov og orden med henblikk på borgernes velferd, og må ikke påvirke det vesentlige innholdet i friheten eller rettigheten (artikkel 37 nr. 2 i forfatningen).

([103]) I artikkel 43 nr. 2 i gjennomføringsdekretet til PIPA er det fastsatt en spesiell prosedyre som gjelder dersom den behandlingsansvarlige behandler personopplysningsfiler som er mottatt fra en annen behandlingsansvarlig.

([104]) Manglende nødvendige tiltak for å korrigere eller slette personopplysninger og fortsatt bruk eller videreformidling av disse opplysningene til en tredjepart kan føre til strafferettslige sanksjoner (artikkel 73 nr. 2 i PIPA).

([105]) I henhold til artikkel 44 nr. 2 i gjennomføringsdekretet til PIPA skal den behandlingsansvarlige underrette den registrerte om at den behandlingsansvarlige har innstilt behandlingen, senest ti dager etter mottak av anmodningen.

([106]) Med hensyn til offentlige institusjoner kan retten til å få innstilt behandlingen utøves når det gjelder opplysninger i registrerte personopplysningsfiler (artikkel 37 sammenholdt med artikkel 32 i PIPA). En slik registrering kreves ikke i et begrenset antall situasjoner, for eksempel når personopplysningsfilene er knyttet til nasjonal sikkerhet, strafferettslig etterforskning, diplomatiske forbindelser osv. (artikkel 32 nr. 2 i PIPA).

([107]) Dersom behandlingen ikke innstilles, kan det føre til strafferettslige sanksjoner (artikkel 73 nr. 3 i PIPA).

([108]) Tvisteløsningsutvalget (se betraktning 133) har behandlet en rekke saker der enkeltpersoner har klaget på bruken av deres opplysninger til direkte markedsføring uten samtykke, som blant annet har ført til at den aktuelle behandlingsansvarlige har betalt erstatning og slettet personopplysninger (se for eksempel tvisteløsningsutvalget 20R10-024(2020.11.18), 20R08-015(2020.8.28), 20R07-031(2020.9.1)).

opplysningene til direkte markedsføring – det vil si det faktum at den registrerte kan bli kontaktet i forbindelse med markedsføring av varer eller tjenester eller bli oppfordret til å kjøpe dem – på en «tydelig og gjenkjennelig måte» (artikkel 22 nr. 2 og 4 i PIPA sammenholdt med artikkel 17 nr. 2 pkt. 1 i gjennomføringsdekretet til PIPA).

80) For å gjøre det enklere å utøve individuelle rettigheter må den behandlingsansvarlige innføre spesifikke prosedyrer og offentliggjøre dem (artikkel 38 nr. 4 i PIPA)([109]). Dette omfatter prosedyrer for å klage på et avslag på en anmodning (artikkel 38 nr. 5 i PIPA). Den behandlingsansvarlige må sikre at framgangsmåten for utøvelse av rettigheter er «brukervennlig for den registrerte» og ikke vanskeligere enn framgangsmåten for innsamling av personopplysningene. Dette omfatter også en forpliktelse til å legge ut informasjon om framgangsmåten på eget nettsted (artikkel 41 nr. 2, artikkel 43 nr. 1 og artikkel 44 nr. 1 i gjennomføringsdekretet til PIPA)([110]). Enkeltpersoner kan gi en representant tillatelse til å inngi en slik anmodning (artikkel 38 nr. 1 i PIPA sammenholdt med artikkel 45 i gjennomføringsdekretet til PIPA). Den behandlingsansvarlige kan kreve et gebyr (og porto dersom det anmodes om at det sendes kopier av personopplysninger), men beløpet skal fastsettes «på grunnlag av de faktiske kostnadene for å behandle [anmodningen]». Det skal ikke kreves gebyr (eller porto) dersom det er den behandlingsansvarlige som er opphavet til anmodningen (artikkel 38 nr. 3 i PIPA sammenholdt med artikkel 47 i gjennomføringsdekretet til PIPA).

81) PIPA og gjennomføringsdekretet til den inneholder ikke generelle bestemmelser om beslutninger som påvirker den registrerte, og som utelukkende er basert på automatisk behandling av personopplysninger. Når det gjelder personopplysninger som er samlet inn i Unionen, vil enhver beslutning som er basert på automatisk behandling, imidlertid vanligvis bli truffet av den behandlingsansvarlige i Unionen (som har en direkte relasjon til den berørte registrerte), og den omfattes derfor av forordning (EU) 2016/679([111]). Dette omfatter overføringsscenarioer der behandlingen utføres av en utenlandsk (for eksempel sørkoreansk) økonomisk operatør som opptrer som agent (databehandler) på vegne av den behandlingsansvarlige i Unionen (eller som en underleverandør som opptrer på vegne av databehandleren i Unionen som har mottatt dataene fra en behandlingsansvarlig i Unionen som har samlet inn opplysningene), og som på dette grunnlaget så treffer beslutningen. Fraværet av særlige regler for automatisert beslutningstaking i PIPA vil derfor sannsynligvis ikke påvirke beskyttelsesnivået for personopplysninger som overføres i henhold til denne beslutningen.

82) Som et unntak får bestemmelsene om åpenhet på anmodning (artikkel 20) og individuelle rettigheter (artikkel 35–37) samt kravet til leverandører av informasjons- og kommunikasjonstjenester om individuell underretning (artikkel 39-8 i PIPA) ikke anvendelse på pseudonymiserte opplysninger når disse behandles for statistiske formål eller for formål knyttet til vitenskapelig forskning eller arkivering i allmennhetens interesse (artikkel 28-7 i PIPA)([112]). I tråd med artikkel 11 nr. 2 (sammenholdt med betraktning 57) i forordning (EU) 2016/679 begrunnes dette i det faktum at den behandlingsansvarlige for å sikre åpenhet eller gi individuelle rettigheter vil måtte identifisere om noen (og i så fall hvilke) av opplysningene er knyttet til personen som inngir anmodningen, noe som er uttrykkelig forbudt i henhold til PIPA (artikkel 28-5 nr. 1 i PIPA). Dersom en slik reidentifisering innebærer at pseudonymiseringen oppheves for hele (det pseudonymiserte) datasettet, vil det utsette alle berørte personers personopplysninger for økte risikoer. Mens det i forordning (EU) 2016/679 vises til situasjoner der reidentifisering er praktisk umulig, er PIPA strengere ved at reidentifisering er uttrykkelig forbudt i alle situasjoner der det behandles pseudonymiserte opplysninger.

83) Det sørkoreanske systemet, som beskrevet i betraktning 74–82), inneholder derfor regler om registrertes rettigheter som gir et beskyttelsesnivå som i det vesentlige tilsvarer nivået fastsatt i forordning (EU) 2016/679.

([109]) Se også artikkel 30 nr. 1 pkt. 5 i PIPA om personvernprogrammet, som blant annet skal inneholde informasjon om den enkeltes rettigheter og om hvordan de utøves.

([110]) Se også artikkel 39-7 nr. 2 i PIPA om leverandører av informasjons- og kommunikasjonstjenester.

([111]) I unntakstilfeller kan det imidlertid finnes en direkte relasjon mellom den sørkoreanske økonomiske operatøren og den registrerte i EU, noe som vanligvis skyldes at vedkommende har målrettet sin innsats mot den aktuelle personen i Den europeiske unionen ved å tilby ham/henne varer eller tjenester eller ved å overvåke hans/hennes atferd. Da vil den sørkoreanske økonomiske operatøren selv være omfattet av virkeområdet for forordning (EU) 2016/679 (artikkel 3 nr. 2) og skal dermed direkte overholde EUs regelverk for vern av personopplysninger.

([112]) Se også melding 2021-5, der det bekreftes at avsnitt III i PIPA (herunder artikkel 28-7) bare får anvendelse når pseudonymiserte opplysninger behandles for statistiske formål eller formål knyttet til vitenskapelig forskning eller arkivering i allmennhetens interesse, se avsnitt 4 i vedlegg I til denne beslutningen.

2.3.9 *Videreoverføring*

84) Beskyttelsesnivået for personopplysninger som overføres fra Unionen til behandlingsansvarlige i Republikken Korea, må ikke undergraves av videreoverføring av slike opplysninger til mottakere i et tredjeland.

85) Slik «videreoverføring» utgjør internasjonale overføringer fra Republikken Korea sett fra den sørkoreanske behandlingsansvarliges ståsted. I denne forbindelse skilles det i PIPA mellom utkontraktering av behandlingen til en underleverandør (det vil si en databehandler) og videreformidling av personopplysninger til tredjeparter([113]).

86) For det første skal den sørkoreanske behandlingsansvarlige, når behandlingen av personopplysninger utkontrakteres til en enhet i et tredjeland, sikre at PIPAs bestemmelser om utkontraktering overholdes (artikkel 26 i PIPA). Dette omfatter innføring av et rettslig bindende instrument som blant annet begrenser underleverandørens behandling til det som er formålet med det utkontrakterte arbeidet, pålegger tekniske og organisatoriske garantier og begrenser den utkontrakterte behandlingen (se artikkel 26 nr. 1 i PIPA), og offentliggjøring av informasjon om det utkontrakterte arbeidet. Den behandlingsansvarlige plikter i tillegg å gi underleverandøren «opplæring» om nødvendige sikkerhetstiltak og å kontrollere, herunder gjennom inspeksjoner, at den behandlingsansvarliges forpliktelser i henhold til PIPA([114]) og utkontrakteringsavtalen overholdes.

87) Dersom underleverandøren forårsaker skade som følge av behandling av personopplysninger i strid med PIPA, holdes den behandlingsansvarlige ansvarlig med henblikk på erstatningsansvaret, det samme gjelder dersom skaden forårsakes av en ansatt hos den behandlingsansvarlige (artikkel 26 nr. 6 i PIPA). Den sørkoreanske behandlingsansvarlige er derfor fortsatt ansvarlig for personopplysningene som er blitt utkontraktert, og må sikre at den utenlandske databehandleren behandler opplysningene i samsvar med PIPA. Dersom underleverandøren behandler opplysningene i strid med PIPA, kan den sørkoreanske behandlingsansvarlige bli holdt ansvarlig for manglende overholdelse av forpliktelsen til å sikre at PIPA overholdes, for eksempel gjennom sin kontroll av underleverandøren. Garantiene i utkontrakteringsavtalen og den sørkoreanske behandlingsansvarliges ansvar for underleverandørens handlinger sikrer kontinuitet i vernet når behandlingen av personopplysninger utkontrakteres til en enhet utenfor Republikken Korea.

88) For det andre kan sørkoreanske behandlingsansvarlige videreformidle personopplysninger til en tredjepart utenfor Republikken Korea. Selv om PIPA inneholder en rekke rettslige grunner som muliggjør videreformidling til tredjeparter generelt, skal den behandlingsansvarlige, dersom tredjeparten befinner seg utenfor Republikken Korea, i prinsippet([115]) innhente den registrertes samtykke([116]) etter å ha gitt den registrerte informasjon om 1) typen personopplysninger, 2) mottakeren av personopplysninger, 3) formålet med overføringen, det vil si formålet med mottakerens behandling, 4) hvor lenge opplysningene vil bli lagret i forbindelse med mottakerens behandling, og 5) og at den registrerte har rett til å nekte å samtykke (artikkel 17 nr. 2 og 3 i PIPA). I avsnittet om åpenhet i melding 2021-5 (se betraktning 70) angis det at enkeltpersoner skal informeres om tredjelandet som deres opplysninger vil bli videreformidlet til. Dette sikrer at registrerte i Unionen kan treffe en fullt ut informert beslutning om hvorvidt de ønsker å samtykke til at opplysningene videreformidles til utlandet. Den behandlingsansvarlige må dessuten ikke inngå en avtale med tredjepartsmottakeren i strid med PIPA, noe som betyr at avtalen ikke må inneholde forpliktelser som strider mot kravene som stilles til den behandlingsansvarlige i henhold til PIPA([117]).

([113]) Det gjelder særlige regler for leverandører av informasjons- og kommunikasjonstjenester. I samsvar med artikkel 39-12 i PIPA må leverandører av informasjons- og kommunikasjonstjenester i prinsippet innhente brukerens samtykke til enhver overføring av personopplysninger til utlandet. Dersom personopplysninger overføres som et ledd i utkontrakteringen av behandlingsaktiviteter, herunder for å bli lagret, kreves det ikke samtykke dersom de aktuelle personene direkte eller ved en lett tilgjengelig offentlig melding på forhånd er blitt informert om 1) opplysningene som skal overføres, 2) landet som opplysningene skal overføres til (samt overføringsdato og -metode), 3) navnet på mottakeren og 4) formålet med mottakerens bruk og lagring (artikkel 39-12 nr. 3 i PIPA). I tillegg får de generelle kravene som gjelder utkontraktering, anvendelse i dette tilfellet. For hver overføring må det finnes spesifikke garantier med hensyn til sikkerhet, behandling av klager og tvister samt andre tiltak som er nødvendige for å beskytte brukernes opplysninger (artikkel 48-10 i gjennomføringsdekretet til PIPA).

([114]) Se også artikkel 26 nr. 7 i PIPA der det er fastsatt at artikkel 15–25, artikkel 27–31, artikkel 33–38 og artikkel 50 gjelder tilsvarende med nødvendige endringer for databehandleren.

([115]) Dersom leverandører av informasjons- og kommunikasjonstjenester videreformidler brukernes personopplysninger til tredjeparter, krever dette alltid brukerens samtykke (artikkel 39-12 nr. 2 i PIPA).

([116]) Som forklart nærmere i fotnote 51 skal et slikt samtykke være gitt frivillig og være informert og spesifikt for å være gyldig.

([117]) Se også artikkel 39-12 nr. 1 i PIPA om leverandører av informasjons- og kommunikasjonstjenester.

89) Personopplysninger kan uten den registrertes samtykke videreformidles til en tredjepart (i utlandet) dersom formålet fremdeles er «innenfor rammer som er rimelig relatert til» det opprinnelige formålet med innsamlingen (artikkel 17 nr. 4 i PIPA, se betraktning 36). Når det skal besluttes om personopplysninger skal utleveres for et «relatert» formål, må den behandlingsansvarlige imidlertid ta hensyn til om dette er til ulempe for den registrerte, og om det er truffet nødvendige sikkerhetstiltak (for eksempel kryptering). Ettersom tredjelandet som personopplysninger overføres til, ikke alltid har et beskyttelsesnivå som svarer til nivået i PIPA, anerkjennes det i avsnitt 2 i melding 2021-5 at slike ulemper kan oppstå og bare kan unngås dersom den sørkoreanske behandlingsansvarlige og den utenlandske mottakeren gjennom et rettslig bindende instrument (for eksempel en avtale) sikrer et beskyttelsesnivå som tilsvarer nivået i PIPA, herunder med hensyn til de registrertes rettigheter.

90) Det gjelder særlige regler for «ikke-formålsmessig» utlevering, det vil si videreformidling av opplysninger til en tredjepart for et nytt (ikke-relatert) formål, som bare kan finnes sted av en av grunnene angitt i artikkel 18 nr. 2 i PIPA, som beskrevet i betraktning 39. Selv under disse omstendighetene er videreformidling til en tredjepart imidlertid unntatt dersom det er sannsynlig at det vil «krenke den registrertes eller tredjepartens interesser urettmessig», noe som krever en avveining av interesser. I henhold til artikkel 18 nr. 5 i PIPA må den behandlingsansvarlige dessuten anvende ytterligere garantier, som kan omfatte å be tredjeparten om å begrense formålet med og metoden for behandlingen eller innføre spesifikke sikkerhetstiltak. Ettersom tredjelandet som personopplysningene overføres til, ikke alltid har et beskyttelsesnivå som svarer til nivået i PIPA, anerkjennes det i avsnitt 2 i melding 2021-5 at en slik «urettmessig krenking av den registrertes eller en tredjeparts interesser» kan oppstå og bare kan unngås dersom den sørkoreanske behandlingsansvarlige og den utenlandske mottakeren gjennom et rettslig bindende instrument (for eksempel en avtale) sikrer et beskyttelsesnivå som svarer til nivået i PIPA, herunder med hensyn til de registrertes rettigheter.

91) Reglene i betraktning 86–90 sørger derfor for en kontinuitet i vernet når personopplysninger videreoverføres (til en «underleverandør» eller en tredjepart) fra Republikken Korea, som i det vesentlige tilsvarer det som er fastsatt i forordning (EU) 2016/679.

2.3.10 *Ansvarlighet*

92) I henhold til prinsippet om ansvarlighet skal enheter som behandler opplysninger, treffe egnede tekniske og organisatoriske tiltak for effektivt å kunne oppfylle sine forpliktelser med hensyn til vern av personopplysninger, og de skal kunne dokumentere at de oppfyller disse forpliktelsene, særlig overfor vedkommende tilsynsmyndighet.

93) I henhold til artikkel 3 nr. 6 og 8 i PIPA må den behandlingsansvarlige behandle personopplysninger «på en måte som minimerer risikoen for å krenke» den registrertes personvern, og bestrebe seg på å få den registrertes tillit ved å overholde og utføre oppgavene og ansvarsområdene angitt i PIPA og andre relaterte lover. Dette omfatter utarbeiding av en intern styringsplan (artikkel 29 i PIPA) og egnet opplæring av og tilsyn med personalet (artikkel 28 i PIPA).

94) Som et middel for å sikre ansvarlighet pålegges behandlingsansvarlige gjennom artikkel 31 i PIPA sammenholdt med artikkel 32 i gjennomføringsdekretet til PIPA å utpeke en personvernansvarlig med «overordnet ansvar for behandlingen av personopplysninger». Denne personvernansvarlige skal særlig ha følgende oppgaver: 1) Utarbeide og gjennomføre en plan for vern av personopplysninger og utarbeide personvernprogrammet, 2) gjennomføre regelmessige undersøkelser om status og praksis for behandling av personopplysninger med henblikk på å utbedre eventuelle mangler, 3) håndtere klager og erstatninger, 4) opprette et internt kontrollsystem for å hindre utlevering, misbruk eller feil bruk av personopplysninger, 5) utarbeide og gjennomføre et opplæringsprogram, 6) verne, kontrollere og håndtere personopplysningsfiler og (7) tilintetgjøre personopplysningene når formålet med behandlingen er oppnådd eller lagringstiden er utløpt. Ved utføring av disse oppgavene kan den personvernansvarlige kontrollere statusen for behandlingen av personopplysninger og relaterte systemer og anmode om informasjon om dette (artikkel 31 nr. 3 i PIPA). Dersom den personvernansvarlige får kjennskap til overtredelser av PIPA eller andre relevante lover for vern av personopplysninger, skal vedkommende umiddelbart treffe korrigerende tiltak og underrette den behandlingsansvarliges ledelse («leder») om disse tiltakene dersom det er nødvendig (artikkel 31 nr. 4 i PIPA). I henhold til artikkel 31 nr. 5 i PIPA må det ikke være forbundet med urimelige ulemper for den personvernansvarlige å utføre disse oppgavene.

95) Behandlingsansvarlige må i tillegg på en proaktiv måte bestrebe seg på å gjennomføre en konsekvensanalyse av følgene for personvernet dersom behandlingen av personopplysningsfiler innebærer en risiko for personvernet (artikkel 33 nr. 8 i PIPA). På grunnlag av artikkel 33 nr. 1 og 2 i PIPA sammenholdt med artikkel 35, 36 og 38 i gjennomføringsdekretet til PIPA vil faktorer som de behandlede opplysningenes type og art (særlig hvorvidt det dreier seg om sensitive opplysninger), volum og hvor lenge de vil bli lagret, samt sannsynligheten for brudd på opplysningssikkerheten være relevante for vurderingen av graden av risiko for de registrertes rettigheter. Formålene med konsekvensanalysen er å sikre at faktorer som utgjør en risiko for personvernet, og eventuelle sikkerhets- eller andre mottiltak analyseres, og å påpeke forhold som må forbedres (se artikkel 33 nr. 1 i PIPA sammenholdt med artikkel 38 i gjennomføringsdekretet til PIPA).

96) Offentlige institusjoner plikter å gjennomføre en konsekvensanalyse ved behandling av visse personopplysningsfiler med høyere risiko for at personvernet krenkes (artikkel 33 nr. 1 i PIPA). I samsvar med artikkel 35 i gjennomførings-dekretet til PIPA gjelder dette blant annet filer som inneholder sensitive opplysninger om minst 50 000 registrerte, filer som vil bli samkjørt med andre filer, og som dermed vil inneholde opplysninger om minst 500 000 registrerte, eller filer som inneholder opplysninger om minst en million registrerte. Resultatet av en konsekvensanalyse utført av en offentlig institusjon må oversendes til PIPC (artikkel 33 nr. 1 i PIPA), som kan avgi uttalelse (artikkel 33 nr. 3 i PIPA).

97) For det tredje er det i artikkel 13 i PIPA fastsatt at PIPC skal utarbeide nødvendige retningslinjer for å fremme og støtte behandlingsansvarliges «selvregulerende aktiviteter knyttet til vern av personopplysninger», blant annet gjennom opplæring om vern av personopplysninger, fremming av og støtte til organisasjoner som arbeider med vern av person-opplysninger, og ved å bistå behandlingsansvarlige med å innføre og gjennomføre selvregulerende regler. PIPC skal dessuten innføre og fremme gjennomføringen av ePRIVACY-symbolsystemet. I denne forbindelse gir artikkel 32-2 i PIPA sammenholdt med artikkel 34-2 til 34-8 i gjennomføringsdekretet til PIPA mulighet for å sertifisere at den behandlingsansvarliges systemer for behandling og vern av personopplysninger oppfyller kravene i PIPA. I henhold til disse reglene kan det gis en sertifisering([118]) (for en periode på tre år) dersom den behandlingsansvarlige oppfyller sertifiseringskriteriene fastsatt av PIPC, herunder fastsettelse av organisatoriske, tekniske og fysiske garantier for å verne personopplysninger([119]). PIPC må minst én gang i året foreta en gjennomgåelse av den behandlingsansvarliges systemer som er relevante for sertifiseringen, for å sikre at de fortsatt er effektive, noe som kan føre til at sertifiseringen tilbakekalles (artikkel 32 nr. 4 i PIPA sammenholdt med artikkel 34-5 i gjennomføringsdekretet til PIPA, såkalt «oppfølgingsstyring»).

98) Den sørkoreanske rammen gjennomfører derfor prinsippet om ansvarlighet på en måte som sikrer et beskyttelsesnivå som i det vesentlige tilsvarer nivået fastsatt i forordning (EU) 2016/679, herunder gjennom innføring av forskjellige mekanismer for å sikre og dokumentere samsvar med PIPA.

2.3.11 *Særlige regler for behandling av personlige kredittopplysninger*

99) Som beskrevet i betraktning 13 er det i CIA fastsatt særlige regler for kommersielle operatørers behandling av personlige kredittopplysninger. Ved behandling av personlige kredittopplysninger skal kommersielle operatører derfor oppfylle de generelle kravene i PIPA, med mindre CIA inneholder mer spesifikke regler. Dette vil for eksempel være tilfellet når de behandler opplysninger knyttet til et kredittkort eller en bankkonto i forbindelse med en kommersiell transaksjon med en enkeltperson. Som sektorlovgivning for behandling av kredittopplysninger (både personlige og ikke-personlige) er det i CIA ikke bare fastsatt spesifikke garantier for vern av opplysninger (for eksempel med tanke på åpenhet og sikkerhet), loven regulerer også mer generelt de spesifikke omstendighetene der personlige kreditt-opplysninger kan behandles. Dette gjenspeiles særlig i de detaljerte kravene til bruk, videreformidling av opplysninger til en tredjepart og lagring av slike opplysninger.

100) I likhet med PIPA gjenspeiler CIA prinsippet om lovlighet og forholdsmessighet. For det første tillater artikkel 15 nr. 1 i CIA som et generelt krav bare at det samles inn personlige kredittopplysninger ved hjelp av rimelige og lovformelige midler og i det minste omfanget som er nødvendig for å oppfylle et bestemt formål, i samsvar med artikkel 3 nr. 1–2 i PIPA. For det andre regulerer CIA spesifikt lovligheten av behandlingen av personlige kredittopplysninger ved å begrense innsamlingen, bruken og videreformidlingen til en tredjepart og generelt knytte disse behandlingsaktivitetene til kravet om den berørte personens samtykke.

([118]) Dersom den behandlingsansvarlige ønsker å vise til eller fremheve sertifiseringen i forbindelse med sin forretningsvirksomhet, kan vedkommende dessuten bruke symbolet for vern av personopplysninger som PIPC har innført. Se artikkel 34-7 i gjennomføringsdekretet til PIPA.

([119]) Siden november 2018 er systemet ISMS-P (Personal Information & Information Security Management System) utviklet, det sertifiserer at behandlingsansvarlige har et omfattende styringssystem.

101) Personlige kredittopplysninger kan samles inn på grunnlag av en av grunnene fastsatt i PIPA eller av spesifikke grunner fastsatt i CIA. Ettersom artikkel 45 i forordning (EU) 2016/679 forutsetter at personopplysninger overføres av en behandlingsansvarlig eller databehandler i Unionen, og ikke omfatter en sørkoreansk behandlingsansvarligs direkte innsamling (for eksempel fra en enkeltperson eller et nettsted), er det bare samtykke og grunnene fastsatt i PIPA som er relevante for denne beslutningen. Disse grunnene omfatter særlig scenarioer der overføringen er nødvendig for å oppfylle en avtale med personen, eller for den sørkoreanske behandlingsansvarliges berettigede interesser (artikkel 15 nr. 1 pkt. 4 og 6 i PIPA)([120]).

102) Når personlige kredittopplysninger er samlet inn, kan de brukes 1) for det opprinnelige formålet som den aktuelle personen har gitt dem (direkte) for([121]), 2) for et formål som er forenlig med det opprinnelige formålet med innsamlingen([122]), 3) for å fastslå om forretningsforholdet som den aktuelle personen har anmodet om, skal opprettes eller opprettholdes([123]), 4) for statistiske formål og formål knyttet til forskning og arkivering i allmennhetens interesse([124]) dersom opplysningene er pseudonymisert ([125]), 5) dersom det innhentes ytterligere samtykke, eller 6) i samsvar med lovgivningen.

103) Dersom en kommersiell operatør ønsker å utlevere personlige kredittopplysninger til en tredjepart, må vedkommende innhente den berørte personens samtykke([126]) etter å ha informert vedkommende om hvem mottakeren av opplysningene er, og formålet med mottakerens behandling, hvilke opplysninger som skal videreformidles, hvor lenge opplysningene vil bli lagret hos mottakeren, og retten til å nekte å gi samtykke (artikkel 32 nr. 1 i CIA og artikkel 28 nr. 2 i gjennomføringsdekretet til CIA)([127]). Dette kravet om samtykke gjelder ikke i spesifikke situasjoner, særlig når personlige kredittopplysninger utleveres([128]) 1) til en underleverandør for utkontrakteringsformål([129]), 2) til en tredjepart i forbindelse med en virksomhetsoverdragelse, fisjon eller fusjon, 3) for statistiske formål og formål knyttet til forskning og arkivering i allmennhetens interesse, dersom opplysningene er pseudonymisert, 4) for et formål som er forenlig med det opprinnelige formålet med innsamlingen, 5) til en tredjepart som bruker opplysningene til å inndrive gjeld fra personen([130]), 6) for å etterkomme en rettskjennelse, 7) til en representant for påtalemyndigheten eller kriminalpolitiet i

([120]) CIA inneholder også andre rettslige grunner for innsamling, det vil si når det kreves ved lov, dersom opplysningene offentliggjøres av en offentlig institusjon i henhold til lovgivningen om informasjonsfrihet, eller dersom opplysningene er tilgjengelige på et sosialt nettverk. For at den kommersielle operatøren skal kunne påberope seg den siste grunnen, må vedkommende kunne vise at innsamlingen skjer innenfor rammen av den registrertes samtykke på grunnlag av en rimelig («objektiv») fortolkning, og idet det tas hensyn til opplysningenes art, hensikten og formålet med å gjøre dem tilgjengelige på det sosiale nettverket, hvorvidt formålet med innsamlingen er «ytterst relevant» for dette formålet, osv. (artikkel 13 i gjennomføringsdekretet til CIA). Som forklart i betraktning 101 vil disse grunnene imidlertid i prinsippet ikke være relevante i et overføringsscenario.

([121]) For eksempel når kredittopplysninger genereres eller videreformidles i forbindelse med en kommersiell transaksjon med den aktuelle personen. Denne grunnen kan imidlertid ikke anvendes for å bruke personlige kredittopplysninger til direkte markedsføring (se artikkel 33 nr. 1 pkt. 3 i CIA).

([122]) For å avgjøre om formålet med bruken er forenlig med det opprinnelige formålet med innsamlingen, må det tas hensyn til følgende faktorer: 1) Forholdet («relevans») mellom de to formålene, 2) måten opplysningene ble samlet inn på, 3) brukens innvirkning på den aktuelle personen og 4) om det er gjennomført egnede sikkerhetstiltak, for eksempel pseudonymisering (jf. artikkel 32 nr. 6 pkt. 9-4 i CIA).

([123]) En behandlingsansvarlig kan for eksempel måtte ta hensyn til personlige kredittopplysninger som vedkommende har mottatt fra en person, for å avgjøre om den aktuelle personens lån skal forlenges.

([124]) Artikkel 33 i CIA sammenholdt med artikkel 32 nr. 6 pkt. 9-2, 9-4 og 10 i CIA.

([125]) Pseudonymisering defineres i artikkel 2 nr. 15 i CIA som behandling av personlige kredittopplysninger på en slik måte at enkeltpersoner ikke lenger kan identifiseres ut fra opplysningene annet enn samkjørt med andre opplysninger. Selv om CIA inneholder spesifikke garantier for behandling av pseudonymiserte opplysninger for statistiske formål og formål knyttet til forskning og arkivering i allmennhetens interesse (artikkel 40-2 i CIA), får disse reglene ikke anvendelse på kommersielle organisasjoner. Det sistnevnte er i stedet underlagt de særlige kravene i avsnitt III i PIPA, som beskrevet i betraktning 42–48. Ved artikkel 40-3 i CIA unntas dessuten behandling av pseudonymiserte kredittopplysninger – for statistiske formål eller formål knyttet til vitenskapelig forskning eller arkivering i allmennhetens interesse – fra kravene om åpenhet og individuelle rettigheter i likhet med unntaket i artikkel 28-7 i PIPA og med forbehold for garantiene i avsnitt III i PIPA som nærmere beskrevet i betraktning 42–48.

([126]) Dette gjelder ikke dersom opplysningene videreformidles til en tredjepart med henblikk på å sikre at de personlige kredittopplysningene er riktige og oppdaterte, så lenge videreformidlingen finner sted innenfor rammene av det opprinnelige formålet med behandlingen (artikkel 32 nr. 1 i CIA). Dette er for eksempel tilfellet når oppdaterte opplysninger videreformidles til et kredittvurderingsbyrå for å sikre at dets registre er riktige.

([127]) Dersom det ikke er praktisk mulig å utlevere ovennevnte opplysninger, kan det være tilstrekkelig å henvise personen til tredjepartsmottakeren, som vil utlevere de nødvendige opplysningene.

([128]) Ettersom CIA ikke spesifikt regulerer utlevering av personlige kredittopplysninger til utlandet, skal slik utlevering være i samsvar med garantiene for videreoverføring fastsatt i melding 2021-5 avsnitt 2.

([129]) Utkontraktering av behandlingen av personlige kredittopplysninger kan bare skje på grunnlag av en skriftlig avtale og i samsvar med kravene i artikkel 26 nr. 1–3 og 5 i PIPA, som beskrevet i betraktning 20 (artikkel 17 i CIA og artikkel 14 i gjennomføringsdekretet til CIA). Underleverandøren kan bare bruke opplysningene innenfor rammen av de utkontrakterte oppgavene, og selskapet som utkontrakterer oppgavene, må innføre spesifikke krav til sikkerhet (for eksempel kryptering) og gi underleverandøren opplæring i hvordan det kan hindres at kredittopplysningene går tapt eller blir stjålet, utlevert, endret eller bringes i fare.

([130]) Se også artikkel 28 nr. 10 pkt. 1, 2 og 6 i gjennomføringsdekretet til CIA.

en nødssituasjon der den aktuelle personens liv er i fare, eller der det kan forventes at vedkommende vil bli utsatt for kroppsskade, og det ikke er tid til å utstede en rettskjennelse([131]), 8) til vedkommende skattemyndigheter for å overholde skattelovgivningen, eller 9) i samsvar med annen lovgivning. Ved utlevering basert på en av disse grunnene må den registreres underrettes om dette på forhånd (artikkel 32 nr. 7 i CIA).

104) CIA regulerer også spesifikt varigheten av behandlingen av personlige kredittopplysninger basert på en av disse grunnene for bruk eller videreformidling til en tredjepart etter at forretningsforholdet med den aktuelle personen er avsluttet([132]). Det er bare opplysninger som var nødvendige for å opprette eller opprettholde dette forholdet, som kan lagres, med forbehold for ytterligere garantier (de må holdes atskilt fra kredittopplysninger som gjelder personer som det pågår et forretningsforhold med, beskyttes av spesifikke sikkerhetstiltak og bare være tilgjengelige for autoriserte personer)([133]). Alle andre opplysninger må slettes (artikkel 17-2 nr. 1 pkt. 2 i gjennomføringsdekretet til CIA). For å avgjøre hvilke data som var nødvendige for forretningsforholdet, må det tas hensyn til forskjellige faktorer, herunder om det ville vært mulig å opprette forholdet uten opplysningene, og om de direkte gjelder varene eller tjenestene som leveres til den aktuelle personen (artikkel 17-2 nr. 2 i gjennomføringsdekretet til CIA).

105) Selv i tilfeller der personlige kredittopplysninger i prinsippet kan lagres etter at forretningsforholdet er avsluttet, må de slettes senest tre måneder etter at det videre formålet med behandlingen er oppnådd([134]), eller under alle omstendigheter etter fem år (artikkel 20-2 i CIA). I et begrenset antall tilfeller kan personlige kredittopplysninger lagres i mer enn fem år, særlig dersom det er nødvendig for å oppfylle en rettslig forpliktelse, dersom det er nødvendig med henblikk på en persons vitale interesser knyttet til liv, legeme eller eiendom, med henblikk på arkivering av pseudonymiserte opplysninger (som er brukt til statistiske formål eller formål knyttet til vitenskapelig forskning eller arkivering i allmennhetens interesse) eller for forsikringsformål (særlig for forsikringsbetalinger eller for å hindre forsikringssvindel)([135]). I disse unntakstilfellene gjelder det spesifikke garantier (for eksempel at personen skal underrettes om den videre bruken, at de lagrede opplysningene skal holdes atskilt fra opplysningene som gjelder personer der et forretningsforhold fremdeles pågår, og at tilgangsrettighetene skal begrenses, se artikkel 17-2 nr. 1–2 i gjennomføringsdekretet til CIA).

106) I CIA presiseres også prinsippene om riktighet og datakvalitet ved at det kreves at personlige kredittopplysninger «registreres, endres og håndteres» på en måte som sikrer at de er riktige og oppdaterte (artikkel 18 nr. 1 i CIA og artikkel 15 nr. 3 i gjennomføringsdekretet til CIA)([136]). Når kommersielle operatører gir kredittopplysninger til visse andre enheter (for eksempel kredittvurderingsbyråer), plikter de også spesifikt å kontrollere at opplysningene er riktige for å sikre at bare riktige opplysninger registreres og håndteres av mottakeren (artikkel 15 nr. 1 i gjennomføringsdekretet til CIA sammenholdt med artikkel 18 nr. 1 i CIA). Mer generelt krever CIA at det føres registre over innsamling, bruk, utlevering til tredjeparter og tilintetgjøring av personlige kredittopplysninger (artikkel 20 nr. 2 i CIA)([137]).

107) Behandlingen av personlige kredittopplysninger er dessuten underlagt spesifikke krav til opplysningssikkerhet. CIA krever særlig at det gjennomfører teknologiske, fysiske og organisatoriske tiltak for å hindre ulovlig tilgang til datasystemer og endring, tilintetgjøring eller enhver annen risiko for de behandlede opplysningene (for eksempel ved hjelp av tilgangskontroll, se artikkel 19 i CIA og artikkel 16 i gjennomføringsdekretet til CIA). Ved utveksling av personlige kredittopplysninger med en tredjepart må det dessuten inngås en avtale der det fastsettes spesifikke sikkerhetstiltak (artikkel 19 nr. 2 i CIA). Dersom det oppstår et brudd på opplysningssikkerheten for personlige kredittopplysninger, må det treffes tiltak for å minimere eventuelle skader, og de berørte personene må underrettes uten opphold (artikkel 39-4 nr. 1–2 i CIA). I tillegg må PIPC informeres om underretningen av de registrerte og tiltakene som er gjennomført (artikkel 39-4 nr. 4 i CIA).

([131]) I så fall må det uten opphold framsettes en begjæring om kjennelse. Dersom kjennelsen ikke utstedes innen 36 timer, må de mottatte opplysningene slettes uten opphold (artikkel 32 nr. 6 pkt. 6 i CIA).

([132]) For eksempel fordi en av partene har utøvd sin oppsigelsesrett fordi avtaleforpliktelser er oppfylt osv., se artikkel 17-2 nr. 5 i gjennomføringsdekretet til CIA.

([133]) Artikkel 20-2 nr. 1 i CIA og artikkel 17-2 nr. 1 pkt. 1 i gjennomføringsdekretet til CIA.

([134]) Denne fristen tar hensyn til at det ofte ikke vil være mulig å slette opplysningene med det samme, ettersom det vanligvis kreves visse trinn (for eksempel at opplysningene som skal slettes, skilles fra andre opplysninger, og at slettingen skjer uten at informasjonssystemenes stabilitet påvirkes) som det tar en viss tid å gjennomføre.

([135]) Artikkel 20-2 nr. 2 i CIA.

([136]) I artikkel 18 nr. 2 i CIA og artikkel 15 nr. 4 i gjennomføringsdekretet til CIA er det fastsatt mer spesifikke regler for dette registreringskravet, for eksempel for registre over opplysninger som kan være til ulempe for en person, for eksempel opplysninger om straffbare forhold eller konkurser.

([137]) Når det gjelder andre ansvarlighetsmekanismer, kreves det i henhold til CIA at visse organisasjoner (for eksempel kooperativer og offentlige selskaper, se artikkel 21 nr. 2 i gjennomføringsdekretet til CIA) skal utpeke en «kredittopplysningsadministrator/-forvalter» som skal ha ansvar for å overvåke samsvar med CIA og utføre den «personvernansvarliges» oppgaver i henhold til PIPA (artikkel 20 nr. 3 og 4 i CIA).

108) I CIA er det også fastsatt spesifikke forpliktelser når det gjelder åpenhet i forbindelse med innhenting av samtykke til bruk og videreformidling av personlige kredittopplysninger (artikkel 32 nr. 4 og artikkel 34-2 i CIA og artikkel 30-3 i gjennomføringsdekretet til CIA), og, mer generelt, før opplysninger videreformidles til en tredjepart (artikkel 32 nr. 7 i CIA)([138]). De registrerte har dessuten på anmodning rett til å få informasjon om bruken og videreformidlingen av egne kredittopplysninger til tredjeparter i de tre årene forut for anmodningen (herunder formålet med og datoene for en slik bruk/videreformidling)([139]).

109) I henhold til CIA har de registrerte også rett til å få innsyn i sine personlige kredittopplysninger (artikkel 38 nr. 1 i CIA) og til å få rettet uriktige opplysninger (artikkel 38 nr. 2–3 i CIA)([140]). I tillegg til den generelle retten til sletting i henhold til PIPA (se betraktning 77) er det i CIA også fastsatt en spesifikk rett til å få slettet personlige kredittopplysninger som er blitt lagret lenger enn periodene angitt i betraktning 104, det vil si fem år (for personlige kredittopplysninger som var nødvendige for å opprette eller opprettholde et forretningsforhold) eller tre måneder (for andre typer personlige kredittopplysninger)([141]). En anmodning om sletting kan unntaksvis avslås dersom ytterligere lagring er nødvendig i tilfellene beskrevet i betraktning 105. Dersom en person anmoder om sletting, men et av unntakene får anvendelse, må spesifikke garantier få anvendelse på de aktuelle kredittopplysningene (artikkel 38-3 nr. 3 i CIA og artikkel 33-3 i gjennomføringsdekretet til CIA). Opplysningene må for eksempel holdes atskilt fra andre opplysninger, bare være tilgjengelige for autoriserte personer og være omfattet av spesifikke sikkerhetstiltak.

110) I tillegg til rettighetene nevnt i betraktning 109 garanteres enkeltpersoner i henhold til CIA en rett til å be en behandlingsansvarlig om å slutte å kontakte dem med henblikk på direkte markedsføring (lovens artikkel 37 nr. 2) og en rett til dataportabilitet. Med hensyn til det sistnevnte har enkeltpersoner i henhold til CIA rett til å be om at deres personopplysninger overføres til dem selv eller til visse tredjeparter (for eksempel finansinstitusjoner eller kredittvurderingsselskaper). De personlige kredittopplysningene må behandles og overføres til tredjeparten i et format som kan behandles av databehandlingsutstyr (for eksempel en datamaskin).

111) I den grad CIA inneholder særlige regler sammenlignet med PIPA mener Kommisjonen derfor at også disse reglene sikrer et beskyttelsesnivå som i det vesentlige tilsvarer nivået fastsatt i forordning (EU) 2016/679.

2.4 **Tilsyn og håndheving**

112) For å sikre at et tilstrekkelig beskyttelsesnivå for personopplysninger garanteres i praksis, bør det finnes en uavhengig tilsynsmyndighet med myndighet til å overvåke og sikre at reglene for vern av personopplysninger overholdes. Denne myndigheten bør være fullt ut uavhengig og upartisk når den utfører sine oppgaver og utøver sin myndighet.

2.4.1 *Uavhengig tilsyn*

113) I Republikken Korea er PIPC den uavhengige myndigheten med ansvar for tilsyn og håndheving av PIPA. PIPC består av en formann, en nestformann og sju kommisjonsmedlemmer. Formannen og nestformannen utnevnes av presidenten etter innstilling fra statsministeren. To av kommisjonsmedlemmene utnevnes av presidenten etter innstilling fra formannen og fem etter innstilling fra nasjonalforsamlingen (av disse utnevnes to etter innstilling fra det politiske partiet som presidenten tilhører, og tre etter innstilling fra de andre politiske partiene (artikkel 7-2 nr. 2 i PIPA), noe som bidrar

([138]) Dette omfatter et generelt krav om underretning (artikkel 32 nr. 7 i CIA) og et spesifikt krav om åpenhet når opplysninger som gjør det mulig å vurdere en persons kredittverdighet, videreformidles til visse enheter, for eksempel kredittvurderingsbyråer og byråer som samler inn kredittopplysninger (artikkel 35-3 i CIA og artikkel 30-3 i gjennomføringsdekretet til CIA), eller dersom et forretningsforhold ikke inngås, eller avsluttes, på grunnlag av personlige kredittopplysninger mottatt fra en tredjepart (artikkel 36 i CIA og artikkel 31 i gjennomføringsdekretet til CIA).

([139]) Artikkel 35 i CIA. Visse kommersielle organisasjoner, for eksempel kooperativer og offentlige selskaper (artikkel 21 nr. 2 i gjennomføringsdekretet til CIA) er underlagt ytterligere krav om åpenhet, for eksempel om å gjøre visse opplysninger offentlig tilgjengelige (artikkel 31 i CIA) og om å informere de registrerte om at deres kredittskår kan bli negativt påvirket når de deltar i finansielle transaksjoner som utgjør en kredittrisiko (artikkel 35-2 i CIA).

([140]) Når det gjelder vilkårene og unntakene fra retten til innsyn og retting, gjelder reglene i PIPA (beskrevet i betraktning 76–77). Dessuten er det fastsatt ytterligere bestemmelser i artikkel 38 nr. 4–8 i CIA og i artikkel 33 i gjennomføringsdekretet til CIA. En kommersiell operatør som har rettet eller slettet uriktige kredittopplysninger, må underrette den registrerte om dette. I tillegg må enhver tredjepart som har fått utlevert disse opplysningene i løpet av de foregående seks månedene, underrettes, og den berørte registrerte må informeres om dette. Dersom en person ikke er tilfreds med behandlingen av en anmodning om å få rettet opplysninger, kan vedkommende inngi en anmodning til PIPC, som kontrollerer den behandlingsansvarliges handlinger og kan ilegge korrigerende tiltak.

([141]) Artikkel 38-3 i CIA.

til å motvirke partiskhet i utnevnelsesprosessen)([142]). Denne prosedyren er i samsvar med kravene som gjelder for utnevnelse av medlemmer av tilsynsmyndigheter i Unionen (artikkel 53 nr. 1 i forordning (EU) 2016/679). Alle kommisjonsmedlemmer må dessuten avstå fra all inntektsbringende næringsvirksomhet og politiske aktiviteter og fra å inneha stillinger innen offentlig forvaltning eller verv i nasjonalforsamlingen (artikkel 7-6 og 7-7 nr. 1 pkt. 3 i PIPA)([143]). Alle kommisjonsmedlemmer omfattes også av særlige regler som hindrer dem i å delta i forhandlinger i tilfelle en mulig interessekonflikt (artikkel 7-11 i PIPA). PIPC bistås av et sekretariat (artikkel 7-13) og kan nedsette underutvalg (bestående av tre kommisjonsmedlemmer) for å håndtere mindre overtredelser og tilbakevendende spørsmål (artikkel 7-12 i PIPA).

114) Hvert medlem av PIPC utnevnes for tre år og kan gjenutnevnes én gang (artikkel 7-4 nr. 1 i PIPA). Kommisjonsmedlemmene kan bare avsettes under særlige omstendigheter, nærmere bestemt dersom de ikke lenger er i stand til å utføre sine oppgaver på grunn av langvarig svekket psykisk eller fysisk funksjonsevne, handler i strid med loven eller oppfyller et av kriteriene for å bli utestengt fra embetet([144]) (artikkel 7-5 i PIPA). Dette gir dem et institusjonelt vern når de utøver sine funksjoner.

115) Mer generelt garanterer artikkel 7 nr. 1 i PIPA uttrykkelig PIPCs uavhengighet, og i henhold til artikkel 7-5 nr. 2 i PIPA skal kommisjonsmedlemmene utføre sine oppgaver på en uavhengig måte og i samsvar med loven og sin samvittighet([145]). De institusjonelle og prosessuelle garantiene som beskrives, herunder med hensyn til utnevnelse og avsettelse av medlemmene, sikrer at PIPC handler fullt ut uavhengig og uten påvirkning eller instrukser utenfra. I egenskap av å være et sentralt forvaltningsorgan legger PIPC dessuten hvert år fram et forslag til eget budsjett (som gjennomgås av finansdepartementet som en del av det samlede statsbudsjettet før det vedtas av nasjonalforsamlingen) og har ansvar for sin egen personalforvaltning. For tiden har PIPC et budsjett på rundt EUR 35 millioner og 154 ansatte (herunder 40 spesialister på informasjons- og kommunikasjonsteknologi, 32 ansatte med fokus på undersøkelser og 40 juridiske eksperter).

116) PIPCs oppgaver og myndighet er hovedsakelig fastsatt i artikkel 7-8 og 7-9 og i artikkel 61-66 i PIPA([146]). PIPCs oppgaver omfatter særlig rådgivning om lover og regler knyttet til vern av personopplysninger, utarbeiding av strategier og retningslinjer for vern av personopplysninger, undersøkelse av overtredelser av individuelle rettigheter, behandling av klager og mekling i tvister, sikring av at PIPA overholdes, sikring av opplæring om og fremming av vern av personopplysninger og utveksling og samarbeid med personvernmyndigheter i tredjeland([147]).

117) På grunnlag av artikkel 68 i PIPA sammenholdt med artikkel 62 i gjennomføringsdekretet til PIPA er visse av PIPCs oppgaver blitt delegert til Republikken Koreas byrå for internett og sikkerhet, nærmere bestemt 1) utdanning og PR, 2) opplæring av spesialister og utarbeiding av kriterier for konsekvensanalyser av følger for personvernet, 3) behandling av anmodninger om utpeking av institusjoner som foretar slike konsekvensanalyser, 4) behandling av anmodninger om indirekte tilgang til personopplysninger som innehas av offentlige myndigheter (artikkel 35 nr. 2 i PIPA), og 5)

([142]) Det er bare personer som oppfyller følgende kriterier, som kan utnevnes til kommisjonsmedlemmer i PIPC: Høyere tjenestemenn med ansvar for personopplysningsspørsmål, tidligere dommere, statsadvokater eller advokater som har praktisert i minst ti år, tidligere ledere med erfaring innen vern av opplysninger som har arbeidet i en offentlig institusjon eller organisasjon i mer enn tre år, eller som er blitt anbefalt av en slik institusjon eller organisasjon, og tidligere assisterende professorer med fagkunnskap på området vern av opplysninger som har arbeidet i minst fem år i en akademisk institusjon (artikkel 7-2 i PIPA).

([143]) Se også artikkel 4-2 i gjennomføringsdekretet til PIPA.

([144]) Se artikkel 7-7 i PIPA der det er angitt at ikke-sørkoreanske borgere og medlemmer av politiske partier ikke kan bli medlemmer av PIPC. Det samme gjelder for personer som har vært gjenstand for visse typer strafferettslige sanksjoner, som er blitt avsatt fra sin stilling som følge av disiplinære tiltak i løpet av de siste fem årene, osv. (artikkel 7-7 i PIPA sammenholdt med artikkel 33 i loven om offentlige tjenestemenn).

([145]) Selv om det i artikkel 7 nr. 2 i PIPA vises til statsministerens generelle myndighet i henhold til artikkel 18 i loven om organisering av regjeringen til – med presidentens godkjenning – å oppheve eller tilbakekalle enhver ulovlig eller urettmessig bestemmelse truffet av et sentralt forvaltningsorgan, gis det ingen slik myndighet når det gjelder PIPCs undersøkelses- og håndhevingsmyndighet (se artikkel 7 nr. 2 pkt. 1 og 2 i PIPA). Ifølge forklaringene framlagt av den sørkoreanske regjeringen er formålet med artikkel 18 i loven om organisering av regjeringen å gi statsministeren mulighet til å handle under ekstraordinære omstendigheter, for eksempel å mekle i en tvist mellom forskjellige statlige organer. Statsministeren har imidlertid aldri benyttet seg av denne myndigheten siden bestemmelsen ble vedtatt i 1963.

([146]) Når det er nødvendig for å kunne utføre oppgavene i henhold til artikkel 7-9 nr. 1 i PIPA, kan PIPC innhente uttalelser fra relevante offentlige tjenestemenn, eksperter på vern av opplysninger, sivilsamfunnsorganisasjoner og relevante økonomiske operatører. PIPC kan dessuten anmode om relevant materiale, komme med anbefalinger om forbedringer og kontrollere om disse gjennomføres (artikkel 7-9 nr. 2–5 i PIPA).

([147]) Se også artikkel 9 i PIPA (treårig masterplan for vern av personopplysninger), artikkel 12 i PIPA (standardretningslinjer for vern av personopplysninger) og artikkel 13 i PIPA (retningslinjer for fremming og støtte av selvregulering).

oppgaven med å anmode om materiale og foreta inspeksjoner i forbindelse med klager som mottas via den såkalte personverntelefontjenesten. I forbindelse med behandlingen av klager via personverntelefontjenesten overfører Republikken Koreas byrå for internett og sikkerhet saken til PIPC eller til påtalemyndigheten dersom det finner at en lovovertredelse har funnet sted. Muligheten for å inngi en klage til personverntelefontjenesten hindrer ikke at enkeltpersoner kan inngi en klage direkte til PIPC eller henvende seg til PIPC dersom de mener at deres klage ikke er blitt tilfredsstillende behandlet av Republikken Koreas byrå for internett og sikkerhet.

2.4.2 *Håndheving, herunder sanksjoner*

118) For å sikre samsvar med PIPA har lovgiveren gitt PIPC både undersøkelses- og håndhevingsmyndighet som omfatter alt fra anbefalinger til overtredelsesgebyrer. Denne myndigheten kompletteres av en ordning med strafferettslige sanksjoner.

119) Når det gjelder undersøkelsesmyndighet, kan PIPC dersom det er mistanke om eller er blitt rapportert om overtredelse av PIPA, eller dersom det er nødvendig for å beskytte registrertes rettigheter mot overtredelser, utføre stedlige kontroller og anmode om alt relevant materiale (for eksempel artikler og dokumenter) fra behandlingsansvarlige (artikkel 63 i PIPA sammenholdt med artikkel 60 i gjennomføringsdekretet til PIPA)([148]).

120) Når det gjelder håndheving, kan PIPC i henhold til artikkel 61 nr. 2 i PIPA gi råd til behandlingsansvarlige om hvordan beskyttelsesnivået for personopplysninger i forbindelse med spesifikke behandlingsaktiviteter kan forbedres. Behandlingsansvarlige må utvise velvilje med tanke på gjennomføringen av slike råd og underrette PIPC om resultatene. Dersom det er rimelig grunn til å anta at det har skjedd en overtredelse av PIPA, og at dette, dersom det ikke treffes tiltak, sannsynligvis vil forårsake skade som det vil være vanskelig å avhjelpe, kan PIPC ilegge korrigerende tiltak (artikkel 64 nr. 1 i PIPA)([149]). I melding 2021-5 avsnitt 5 (vedlegg I) presiseres det, med bindende virkning, at disse vilkårene er oppfylt når det gjelder overtredelse av noen av bestemmelsene i PIPA som verner enkeltpersoners rett til personvern med hensyn til personopplysninger([150]). Tiltakene som PIPC har myndighet til å treffe, omfatter å kreve at atferden som forårsaket overtredelsen, opphører, midlertidig innstilling av behandlingen eller andre nødvendige tiltak. Manglende overholdelse av korrigerende tiltak kan føre til sanksjoner i form av overtredelsesgebyrer på opptil KRW 50 millioner (artikkel 75 nr. 2 pkt. 13 i PIPA).

121) Når det gjelder visse offentlige myndigheter (for eksempel nasjonalforsamlingen, sentrale forvaltningsorganer, lokale myndigheter og domstolene), er det i artikkel 64 nr. 4 i PIPA fastsatt at PIPC kan «anbefale» de korrigerende tiltakene nevnt i betraktning 120, og at disse myndighetene skal følge en slik anbefaling, med mindre det foreligger ekstraordinære omstendigheter. I henhold til melding 2021-5 avsnitt 5 gjelder dette ekstraordinære faktiske eller rettslige omstendigheter som PIPC ikke hadde kjennskap til da anbefalingen ble utstedt. Den berørte offentlige myndigheten kan bare påberope seg slike ekstraordinære omstendigheter dersom den tydelig dokumenterer at det ikke har skjedd en overtredelse, og PIPC fastslår at dette ikke er tilfellet. Den offentlige myndigheten skal ellers følge PIPCs anbefaling og «treffe et korrigerende tiltak, herunder å stoppe handlingen umiddelbart, og gi skadeserstatning i de unntakstilfellene der det likevel er begått en ulovlig handling».

122) PIPC kan også anmode andre forvaltningsorganer med særlig kompetanse i henhold til sektorlovgivning (for eksempel innen helse, utdanning) om å undersøke – alene eller sammen med PIPC – (antatte) krenkinger av personvernet begått av behandlingsansvarlige som opererer i sektorene som inngår i organenes myndighetsområde, og om at det treffes korrigerende tiltak (artikkel 63 nr. 4–5 i PIPA). I så fall skal PIPC fastsette grunnlaget for, formålet med og omfanget av undersøkelsen([151]). Det berørte forvaltningsorganet må deretter framlegge en inspeksjonsplan for PIPC og underrette PIPC om resultatene av inspeksjonen. PIPC kan anbefale at det treffes et spesifikt korrigerende tiltak, som det berørte organet må bestrebe seg på å gjennomføre. En slik anmodning begrenser under ingen omstendigheter PIPCs myndighet til selv å foreta undersøkelser eller ilegge sanksjoner.

([148]) PIPC har dessuten rett til å få adgang til den behandlingsansvarliges lokaler for å kontrollere statusen for forretningsvirksomheten, registre, dokumenter osv. (artikkel 63 nr. 2 i PIPA). Se også artikkel 45-3 i CIA og artikkel 36-4 i gjennomføringsdekretet til CIA med hensyn til PIPCs myndighet i henhold til den loven.

([149]) Se også artikkel 45-4 i CIA med hensyn til PIPCs myndighet i henhold til CIA.

([150]) I avsnitt 5 i meldingen presiseres det at «vektige grunner til å anta at det har skjedd en overtredelse i forbindelse med personopplysninger, og at det, dersom det ikke treffes tiltak, sannsynligvis vil forårsake skade som det vil være vanskelig å avhjelpe i betydningen angitt i artikkel 64 nr. 1 og 2 i 64 PIPA, gjelder en overtredelse av noen av prinsippene, rettighetene og pliktene som er fastsatt i loven for å verne den enkeltes rett til personopplysninger». Det samme gjelder PIPCs myndighet i henhold til artikkel 45-4 i CIA.

([151]) Artikkel 60 i gjennomføringsdekretet til PIPA.

123) I tillegg til sin myndighet til å treffe korrigerende tiltak kan PIPC ilegge overtredelsesgebyrer på KRW 10–50 millioner for manglende overholdelse av forskjellige krav i PIPA (artikkel 75 i PIPA)([152]). Dette omfatter blant annet manglende overholdelse av kravene som gjelder behandlingens lovlighet, at de nødvendige sikkerhetstiltakene ikke treffes, manglende underretning av registrerte i tilfelle brudd på opplysningssikkerheten, manglende oppfyllelse av kravene som gjelder utkontraktert behandling, manglende utarbeiding og offentliggjøring av et personvernprogram, manglende utpeking av en personvernansvarlig eller å ikke etterkomme en anmodning fra en registrert som utøver sine individuelle rettigheter, samt visse prosessuelle overtredelser (manglende samarbeid i forbindelse med en undersøkelse). Dersom den samme behandlingsansvarlige overtrer flere bestemmelser i PIPA, kan det ilegges et overtredelsesgebyr for hver overtredelse, og ved fastsettelse av gebyrets størrelse vil det bli tatt hensyn til antall berørte personer som påvirkes.

124) Dersom det er rimelig grunn til å mistenke at det har skjedd en overtredelse av PIPA eller andre «lover knyttet til vern av opplysninger», kan PIPC dessuten anmelde forholdet til vedkommende etterforskningsorgan (for eksempel en påtalemyndighet, se artikkel 65 nr. 1 i PIPA). PIPC kan dessuten anbefale den behandlingsansvarlige å treffe disiplinære tiltak overfor den ansvarlige personen (herunder ansvarlig leder, se artikkel 65 nr. 2 i PIPA). Etter å ha mottatt en slik anbefaling må den behandlingsansvarlige følge([153]) anbefalingen og underrette PIPC skriftlig om resultatet (artikkel 65 i PIPA sammenholdt med artikkel 58 i gjennomføringsdekretet til PIPA).

125) Når det gjelder anbefalinger i henhold til artikkel 61, korrigerende tiltak i henhold til artikkel 64, anklager eller anbefalinger om disiplinære tiltak i henhold til artikkel 65 og ilegging av overtredelsesgebyr i henhold til artikkel 75 i PIPA, kan PIPC offentliggjøre fakta – det vil si informasjon om overtredelsen, enheten som har overtrådt loven, og tiltakene som skal treffes – på sitt nettsted eller i en allmenn riksdekkende dagsavis (artikkel 66 i PIPA sammenholdt med artikkel 61 nr. 1 i gjennomføringsdekretet til PIPA) ([154]).

126) Overholdelsen av kravene om vern av opplysninger i PIPA (samt andre «lover knyttet til vern av opplysninger») støttes av en ordning med strafferettslige sanksjoner. I denne forbindelse inneholder artikkel 70–73 i PIPA bestemmelser om sanksjoner som enten kan føre til overtredelsesgebyrer (KRW 20–100 millioner) eller fengsel (med en maksimumsstraff på 2–10 år). Relevante overtredelser omfatter blant annet bruk av personopplysninger eller videreformidling av slike opplysninger til en tredjepart uten nødvendig samtykke, behandling av sensitive opplysninger i strid med forbudet i artikkel 23 nr. 1 i PIPA, manglende overholdelse av gjeldende sikkerhetskrav som fører til at personopplysninger går tapt, blir stjålet, utlevert, forfalsket, endret eller skadet, at det ikke treffes nødvendige tiltak for å rette eller slette personopplysninger eller innstille bruken av dem, eller ulovlig overføring av personopplysninger til et tredjeland([155]). I henhold til artikkel 74 i PIPA er den behandlingsansvarliges ansatte, agent eller representant og den behandlingsansvarlige selv ansvarlig i hvert av disse tilfellene([156]).

127) I tillegg til de strafferettslige sanksjonene som er fastsatt i PIPA, kan misbruk av personopplysninger også utgjøre et straffbart forhold i henhold til straffeloven. Dette er særlig tilfellet ved brudd på konfidensialiteten når det gjelder brev, dokumenter eller elektroniske registre (artikkel 316), utlevering av opplysninger som omfattes av taushetsplikt (artikkel 317), bedrageri ved bruk av datamaskiner (artikkel 347-2) samt underslag og tillitsbrudd (artikkel 355).

128) Det sørkoreanske systemet består derfor av en kombinasjon av forskjellige typer sanksjoner, fra korrigerende tiltak og overtredelsesgebyrer til strafferettslige sanksjoner, som sannsynligvis vil ha en betydelig avskrekkende virkning på behandlingsansvarlige og personer som håndterer opplysningene. PIPC begynte å bruke sin myndighet umiddelbart etter

([152]) Dersom en behandlingsansvarligs systemer for behandling og vern av personopplysninger er blitt sertifisert som forenlig med PIPA, men sertifiseringskriteriene i henhold til artikkel 34-2 nr. 1 i gjennomføringsdekretet til PIPA rent faktisk ikke er oppfylt, eller ved en alvorlige overtredelse av enhver «lov om vern av [person]opplysninger» kan PIPC tilbakekalle sertifiseringen (artikkel 32-2 nr. og 3 og 5 i PIPA). PIPC skal underrette den behandlingsansvarlige om en slik tilbakekalling og skal kunngjøre eller offentliggjøre dette på sitt nettsted eller i det offisielle kunngjøringsbladet (artikkel 34-4 i gjennomføringsdekretet til PIPA). Det er også fastsatt overtredelsesgebyrer (artikkel 52 i CIA) og strafferettslige sanksjoner (artikkel 50 i CIA) for overtredelser av CIA.

([153]) I henhold til artikkel 58 nr. 2 i gjennomføringsdekretet til PIPA skal den behandlingsansvarlige dersom særlige omstendigheter gjør det «praktisk umulig» å følge anbefalingen, gi PIPC en behørig begrunnelse.

([154]) Når PIPC treffer beslutning om en slik offentliggjøring, skal det tas hensyn til overtredelsens innhold og alvorlighetsgrad, dens varighet og hyppighet samt konsekvensene av den (skadens omfang). Den berørte enheten skal underrettes på forhånd og gis mulighet til å forsvare seg. Se artikkel 61 nr. 2 og 3 i gjennomføringsdekretet til PIPA.

([155]) Se artikkel 71 pkt. 2 sammenhold med artikkel 18 nr. 1 i PIPA (manglende overholdelse av vilkårene i artikkel 17 nr. 3 i PIPA som artikkel 18 nr. 1 viser til). Se også artikkel 75 nr. 2 pkt. 1 sammenholdt med artikkel 17 nr. 2 i PIPA (unnlatelse av å gi den berørte personen de nødvendige opplysningene i henhold til artikkel 17 nr. 2 i PIPA som artikkel 17 nr. 3 viser til).

([156]) Artikkel 74-2 i PIPA gir dessuten mulighet til å ta beslag i penger, varer eller andre inntekter som er ervervet som følge av overtredelsen, eller, dersom beslaglegging ikke er mulig, å «inndrive» den ulovlig oppnådde vinningen.

opprettelsen i 2020. Ifølge PIPCs årsrapport for 2021 har PIPC allerede utstedt en rekke anbefalinger, overtredelsesgebyrer og pålegg om korrigerende tiltak, både overfor den offentlige sektor (rundt 34 offentlige myndigheter) og private operatører (rundt 140 selskaper)([157]). Blant saker å merke seg er for eksempel ilegging av et overtredelsesgebyr på KRW 6,7 milliarder i desember 2020 til et selskap for manglende overholdelse av forskjellige bestemmelser i PIPA (herunder sikkerhetskrav, krav til samtykke for videreformidling til tredjeparter og åpenhet)([158]) og et overtredelsesgebyr på KRW 103,3 millioner i april 2021 til et AI-teknologiselskap (blant annet for manglende overholdelse av reglene som gjelder behandlingens lovlighet, særlig samtykke, og behandling av pseudonymiserte opplysninger)([159]). I august 2021 sluttførte PIPC en annen undersøkelse av aktivitetene til tre selskaper som førte til korrigerende tiltak og overtredelsesgebyrer på opptil KRW 6,47 milliarder (blant annet for manglende underretning av enkeltpersoner om utlevering av personopplysninger til tredjeparter, herunder overføring til tredjeland)([160]). Allerede før den nylige reformen hadde Republikken Korea gode resultater når det gjelder håndheving, og de ansvarlige myndighetene benyttet seg av hele spekteret av håndhevingstiltak, herunder overtredelsesgebyrer, korrigerende tiltak og offentliggjøring av navnene på en rekke behandlingsansvarlige, herunder leverandører av kommunikasjonstjenester (Republikken Koreas kommunikasjonskommisjon) og kommersielle operatører, finansinstitusjoner, offentlige myndigheter, universiteter og sykehus (innenriks- og sikkerhetsdepartementet)([161]). På dette grunnlaget konkluderer Kommisjonen med at Republikken Koreas system sikrer en effektiv håndheving av reglene for vern av personopplysninger i praksis, og dermed sikrer et beskyttelsesnivå som i det vesentlige tilsvarer det som er fastsatt i forordning (EU) 2016/679.

2.5 **Prøvings- og klageadgang**

129) For å sikre tilstrekkelig vern, særlig håndheving av individuelle rettigheter, bør den registrerte få mulighet til effektiv administrativ og rettslig prøving, herunder skadeserstatning.

130) Det sørkoreanske systemet gir enkeltpersoner adgang til forskjellige mekanismer som de kan bruke for effektivt å utøve sine rettigheter og få adgang til (rettslig) prøving.

131) Som et første trinn kan personer som mener at deres rettigheter eller interesser med hensyn til vern av opplysninger er blitt krenket, henvende seg til den relevante behandlingsansvarlige. I henhold til artikkel 30 nr. 1 pkt. 5 i PIPA skal den behandlingsansvarliges personvernprogram blant annet inneholde informasjon om de registrertes rettigheter og om hvordan de kan utøves. Det skal dessuten inneholde kontaktopplysninger, for eksempel navnet på og telefonnummeret til den personvernansvarlige eller avdelingen med ansvar for vern av opplysninger, for å gjøre det mulig å inngi klager. I den behandlingsansvarliges organisasjon er det den personvernansvarliges oppgave å behandle klager, treffe korrigerende tiltak ved krenking av personvernet og håndtere erstatninger (artikkel 31 nr. 2 pkt. 3 og 4 i PIPA). Det sistnevnte gjelder for eksempel ved et brudd på opplysningssikkerheten, ettersom den behandlingsansvarlige blant annet skal underrette den registrerte om det eller de kontaktpunktene for rapportering av skade (artikkel 34 nr. 1 pkt. 5 i PIPA).

132) I henhold til PIPA har enkeltpersoner dessuten en rekke muligheter til å få prøvet sin sak mot behandlingsansvarlige. For det første kan enhver person som mener at den behandlingsansvarlige har krenket deres rettigheter eller interesser med hensyn til vern av opplysninger, rapportere slike overtredelser direkte til PIPC og/eller til en av de spesialiserte institusjonene som PIPC har utpekt for å motta og håndtere klager, herunder Republikken Koreas byrå for internett og sikkerhet, som for dette formålet driver en telefontjeneste (den såkalte personverntelefontjenesten) (artikkel 62 nr.1 og 2 i PIPA sammenholdt med artikkel 59 i gjennomføringsdekretet til PIPA). Personverntelefontjenesten undersøker og

([157]) Se s. 50–55 i PIPCs årsrapport for 2021 (bare tilgjengelig på koreansk): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK

([158]) Se (bare tilgjengelig på koreansk): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Se (bare tilgjengelig på koreansk): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Se (bare tilgjengelig på koreansk): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Se for eksempel årsrapporten for 2020 (bare tilgjengelig på koreansk) på https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 og eksemplene gitt på engelsk på https://www.privacy.go.kr/eng/enforcement_02.do.

fastslår overtredelser, gir råd i forbindelse med behandling av personopplysninger (artikkel 62 nr. 3 i PIPA) og kan rapportere overtredelser til PIPC (men kan ikke selv treffe håndhevingstiltak). Personverntelefontjenesten mottar et stort antall klager/henvendelser (for eksempel 177 457 i 2020, 159 255 i 2019 og 164 497 i 2018)([162]). I henhold til informasjon framlagt av PIPC mottok PIPC rundt 1 000 klager i perioden mellom august 2020 og august 2021. Som svar på en klage kan PIPC utstede anbefalinger om forbedringer eller korrigerende tiltak, sende en «anklage» til vedkommende etterforskningsorgan (herunder en påtalemyndighet) eller utstede anbefalinger om disiplinære tiltak (se artikkel 61, 64 og 65 i PIPA). PIPCs beslutninger (for eksempel avslag på å behandle en klage eller avslag på en klage) kan bestrides i henhold til forvaltningsprosessloven([163]).

133) For det andre kan registrerte i henhold til artikkel 40–50 i PIPA sammenholdt med artikkel 48-14–57 i gjennomføringsdekretet til PIPA klage til et såkalt tvisteløsningsutvalg som består av representanter utpekt av formannen for PIPC blant medlemmene av kommisjonens øverste ledelse, og av enkeltpersoner som utpekes på grunnlag av erfaring innen vern av opplysninger blant visse grupper (se artikkel 40 nr. 2, 3 og 7 i PIPA og artikkel 48-14 i gjennomføringsdekretet til PIPA)([164]). Muligheten til å benytte seg av mekling i tvisteløsningsutvalget er en alternativ klageadgang, men begrenser ikke den enkeltes rett til å klage til PIPC eller gå til domstolene. I forbindelse med behandlingen av saken kan utvalget anmode partene i tvisten om å framlegge det nødvendige materialet og/eller innkalle relevante vitner til å møte for utvalget (artikkel 45 i PIPA). Når saken er avklart, utarbeider utvalget et meklingsforslag([165]) som skal støttes av et flertall blant utvalgets medlemmer. Meklingsforslaget kan omfatte krav om at overtredelsen skal stoppe, nødvendige avhjelpende tiltak (herunder restitusjon eller erstatning) og eventuelle tiltak som er nødvendige for å hindre at de samme eller lignende overtredelser gjentar seg (artikkel 47 nr. 1 i PIPA). Dersom begge parter godtar meklingsforslaget, vil det ha samme virkning som et rettsforlik (artikkel 47 nr. 5 i PIPA). Ingen av partene hindres i å bringe saken inn for domstolene mens en mekling pågår, i så fall innstilles meklingen (se artikkel 48 nr. 2 i PIPA)([166]). De årlige tallene framlagt av PIPC viser at enkeltpersoner regelmessig benytter seg av prosedyren ved tvisteløsningsutvalget, og at dette ofte fører til et positivt resultat. I 2020 behandlet utvalget for eksempel 126 saker, hvorav 89 ble løst i utvalget (i 77 av sakene nådde partene enighet allerede før meklingsprosessen var ferdig, og i 12 saker godtok partene meklingsforslaget), noe som innebærer en forliksgrad på 70,6 %([167]). I 2019 behandlet utvalget 139 saker. hvorav 92 ble løst, noe som innebærer en forliksgrad på 62,2 %.

134) Dersom minst 50 personer blir skadelidende, eller dersom deres rettigheter med henblikk på vern av opplysninger er blitt krenket på samme eller lignende måte som følge av samme (type) hendelse([168]), kan en registrert eller en personvernorganisasjon søke om kollektiv mekling på vegne av en slik gruppe. Andre registrerte kan søke om å delta i en slik mekling, som vil bli offentliggjort av tvisteløsningsutvalget (artikkel 49 nr. 1–3) i PIPA sammenholdt med artikkel 52–54 i gjennomføringsdekretet til PIPA)([169]). Tvisteløsningsutvalget kan velge minst én person som best

([162]) Se s. 174 i PIPCs årsrapport for 2021. I 2020 gjaldt slike klager for eksempel innsamling av opplysninger uten samtykke, manglende overholdelse av kravene om åpenhet, databehandleres overtredelser av PIPA, utilstrekkelige sikkerhetstiltak, manglende svar på henvendelser fra registrerte samt generelle forespørsler.

([163]) Enkeltpersoner kan særlig påklage et forvaltningsorgans utøvelse av, eller avvisning av å utøve, offentlig myndighet (artikkel 2 nr. 1 pkt. 1 og artikkel 3 pkt. 1 i forvaltningsprosessloven). Betraktning 181 inneholder nærmere opplysninger om prosessuelle aspekter, herunder kravene til hva som kan behandles.

([164]) Alle medlemmene har en fast mandatperiode og kan bare avsettes dersom det foreligger skjellige grunner (se artikkel 40 nr. 5 og artikkel 41 i PIPA). Artikkel 42 i PIPA inneholder dessuten garantier med henblikk på å unngå interessekonflikter.

([165]) Se artikkel 44 i PIPA. I tillegg kan det foreslå et utkast til forlik og anbefale forlik uten mekling (se artikkel 46 i PIPA).

([166]) Utvalget kan i tillegg avvise mekling dersom det anser det som uhensiktsmessig å mekle i tvisten i betraktning av tvistens art, eller fordi formålet som anmodningen om mekling gjelder, er urettmessig (artikkel 48 i PIPA).

([167]) Se s. 179–180 i PIPCs årsrapport for 2021. Disse sakene gjaldt blant annet overtredelser av kravet om å innhente samtykke til innsamling av opplysninger, prinsippet om formålsbegrensning og de registrertes rettigheter.

([168]) Se artikkel 49 nr. 1 i PIPA der det er angitt at registrerte må lide skade eller få sine rettigheter krenket «på samme eller lignende måte», og artikkel 52 pkt. 2 i gjennomføringsdekretet til PIPA, der det er angitt som vilkår at «[v]iktige aspekter av hendelsen faktisk eller rettslig er de samme».

([169]) Dessuten kan tredjeparter også dra nytte av en avgjørelse ved kollektiv mekling som godtas av den behandlingsansvarlige, ettersom tvisteløsningsutvalget kan gi den behandlingsansvarlige råd om å utarbeide og framlegge en plan for erstatning som (også) omfatter dem (artikkel 49 nr. 5 i PIPA).

ivaretar den felles interessen som representativ part (artikkel 49 nr. 4 i PIPA). Dersom den behandlingsansvarlige avslår kollektiv mekling eller ikke godtar meklingsforslaget, kan visse organisasjoner([170]) anlegge et kollektivt søksmål for å få behandlet overtredelsen (artikkel 51–57 i PIPA).

135) For det tredje har den registrerte ved krenking av personvernet som forårsaker «skade» for vedkommende, rett til egnet prøving i en «rask og rettferdig prosedyre» (artikkel 4 pkt. 5 sammenholdt med artikkel 39 i PIPA)([171]). Den behandlingsansvarlige kan bevise sin uskyld ved å dokumentere at det ikke er begått feil («forsettlig» eller ved uaktsomhet). Dersom den registrerte lider skade som følge av tap, tyveri, utlevering, forfalsking eller endring av eller skade på vedkommendes personopplysninger, kan domstolen fastsette en erstatning på opptil tre ganger den faktiske skaden, idet det tas hensyn til en rekke faktorer (artikkel 39 nr. 3 og 4 i PIPA). Alternativt kan den registrerte kreve en «rimelig» erstatning som ikke overstiger KRW 3 millioner (artikkel 39-2 nr. 1 og 2 i PIPA). I henhold til sivilloven kan det dessuten kreves erstatning fra enhver person «som forårsaker tap for eller påfører en annen person skade som følge av en ulovlig handling begått forsettlig eller uaktsomt»([172]), eller fra en person «som har skadet en annen person eller dennes frihet eller omdømme, eller som har påført en annen person en eller annen form for psykiske plager»([173]). Et slikt ansvar utenfor kontraktsforhold som følge av overtredelse av reglene for vern av opplysninger er blitt bekreftet av høyesterett([174]). Dersom en skade er forårsaket av en offentlig myndighets ulovlige handlinger, kan det dessuten inngis et krav om erstatning i henhold til loven om statlig erstatning([175]). Et krav i henhold til loven om statlig erstatning kan inngis til et spesialisert «erstatningsråd» eller direkte til de sørkoreanske domstolene([176]). Statens erstatningsansvar omfatter også skader av ikke-økonomisk art (for eksempel lidelse av psykisk art)([177]). Dersom offeret er en fremmed statsborger, får loven om statlig erstatning anvendelse så lenge vedkommendes opprinnelsesland også sikrer statlig erstatning for sørkoreanske borgere([178]).

136) For det fjerde har høyesterett anerkjent at enkeltpersoner har rett til å kreve at det utstedes et rettslig pålegg ved krenking av deres forfatningsmessige rettigheter, herunder retten til vern av personopplysninger([179]). I denne forbindelse kan en domstol for eksempel pålegge behandlingsansvarlige å innstille eller stanse enhver ulovlig aktivitet. Retten til vern av opplysninger, herunder rettighetene som beskyttes av PIPA, kan dessuten håndheves via sivile søksmål. Høyesterett har anerkjent denne horisontale anvendelsen av den forfatningsmessige beskyttelsen av personvernet på forhold mellom private parter([180]).

([170]) Det vil si forbrukergrupper eller ideelle ikke-statlige organisasjoner med et visst antall medlemmer som har vern av opplysninger som erklært formål (når det gjelder de sistnevnte, kreves det dessuten at minst 100 registrerte som har opplevd samme (type) overtredelse, har inngitt en anmodning om anleggelse av et kollektivt søksmål). Se artikkel 51 i PIPA.

([171]) I artikkel 43–43-3 i CIA er det også fastsatt et erstatningsansvar for skader som følge av overtredelser av den loven.

([172]) Artikkel 750 i sivilloven.

([173]) Artikkel 751 nr. 1 i sivilloven.

([174]) Se for eksempel høyesteretts avgjørelse 2015Da251539, 251546, 251553, 251560, 251577 av 30. mai 2018. Høyesterett har dessuten bekreftet at brudd på opplysningssikkerheten kan føre til rett til skadeserstatning i henhold til sivilloven, se høyesteretts avgjørelse 2011Da59834, 59858, 59841 av 26. desember 2012 (engelsk sammendrag er tilgjengelig på http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). I denne saken presiserte høyesterett at for å vurdere om en person har lidd emosjonell overlast som kan anses som en skade som gir rett til erstatning, bør det tas hensyn til en rekke faktorer, for eksempel typen av opplysninger som er lekket, i hvilken grad personen kan identifiseres som følge av bruddet, muligheten for at tredjeparter kan få tilgang til opplysningene, i hvilken grad personopplysningene er blitt spredd, om dette har ført til ytterligere krenking av individuelle rettigheter, hvordan personopplysningene ble håndtert og beskyttet, osv.

([175]) På grunnlag av loven om statlig erstatning kan enkeltpersoner søke om erstatning for skader som offentlige tjenestemenn forårsaker dersom de utøver sine offisielle arbeidsoppgaver i strid med loven (artikkel 2 nr. 1 i loven).

([176]) Artikkel 9 og 12 i loven om statlig erstatning. Ved loven opprettes det distriktsråd (ledet av visestatsadvokaten ved det aktuelle statsadvokatkontoret), et sentralråd (ledet av visejustisministeren) og et spesialråd (med ansvar for krav om erstatning for skade forårsaket av militært personell eller sivilt ansatte i militæret, ledet av viseforsvarsministeren). Erstatningskrav behandles i prinsippet av distriktsråd, som under visse omstendigheter skal videresende saker til sentral-/spesialrådet, for eksempel dersom erstatningen overstiger et visst beløp, eller dersom en person anmoder om ny behandling. Alle rådene består av medlemmer utpekt av justisministeren (for eksempel blant offentlige tjenestemenn ved justisdepartementet, domstoler, advokater og personer med ekspertise innen statlig erstatning) og omfattes av særlige regler som gjelder interessekonflikter (se artikkel 7 i gjennomføringsdekretet til loven om statlig erstatning).

([177]) Se artikkel 8 i loven om statlig erstatning (som viser til sivilloven) og artikkel 751 i sivilloven.

([178]) Artikkel 7 i loven om statlig erstatning.

([179]) Høyesteretts avgjørelse 93Da40614 av 12. april 1996 og avgjørelse 2008Da42430 av 2. september 2011 (engelsk sammendrag er tilgjengelig på https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Se for eksempel høyesteretts avgjørelse 2008Da42430 av 2. september 2011 (engelsk sammendrag er tilgjengelig på https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

137) For det femte kan enkeltpersoner i henhold til straffeprosessloven (artikkel 223) anmelde et forhold til en statsadvokat eller til kriminalpolitiet([181]).

138) I det sørkoreanske systemet er det derfor forskjellige klagemuligheter, fra lett tilgjengelige og rimelige alternativer (for eksempel ved å kontakte personverntelefontjenesten eller gjennom (kollektiv) mekling) til administrative (ved PIPC) og rettslige midler, herunder muligheten til å oppnå skadeserstatning.

3. SØRKOREANSKE OFFENTLIGE MYNDIGHETERS TILGANG TIL OG BRUK AV PERSONOPPLYSNINGER SOM ER OVERFØRT FRA DEN EUROPEISKE UNION

139) Kommisjonen har også vurdert begrensningene og garantiene, herunder mekanismene for tilsyn og individuell prøvings-/klageadgang i sørkoreansk rett med hensyn til sørkoreanske offentlige myndigheters innsamling og senere bruk av personopplysninger som er overført til behandlingsansvarlige i Republikken Korea i allmennhetens interesse, særlig for formål knyttet til strafferettslig håndheving og nasjonal sikkerhet («offentlige myndigheters tilgang»). I forbindelse med dette har Kommisjonen mottatt offisielle redegjørelser, garantier og forpliktende tilsagn fra den sørkoreanske regjeringen som er undertegnet på høyeste minister- og forvaltningsnivå, og som er angitt i vedlegg II til denne beslutningen.

140) Ved vurderingen av om vilkårene for offentlige myndigheters tilgang til opplysninger som overføres til Republikken Korea i henhold til denne beslutningen, oppfyller «vesentlighetskriteriet» i henhold til artikkel 45 nr. 1 i forordning (EU) 2016/679, som fortolket av Den europeiske unions domstol ut fra Den europeiske unions pakt om grunnleggende rettigheter, har Kommisjonen tatt særlig hensyn til kriteriene angitt nedenfor.

141) For det første skal enhver begrensning av retten til vern av personopplysninger fastsettes ved lov, og i det rettslige grunnlaget som tillater inngrep i en slik rett, skal omfanget av begrensningen på utøvelsen av den aktuelle rettigheten defineres([182]).

142) For det andre skal det, for å oppfylle kravet om forholdsmessighet, som innebærer at unntak fra og begrensninger i vernet av personopplysninger får anvendelse bare i den grad det er strengt nødvendig i et demokratisk samfunn for å nå særskilte mål av allmenn interesse som tilsvarer de som er anerkjent av Unionen, fastsettes klare og presise regler for omfanget og anvendelsen av de aktuelle tiltakene og innføres minstekrav til vern i lovgivningen i det aktuelle tredjelandet som tillater inngrep, slik at personer som får personopplysningene sine overført, har tilstrekkelige garantier for at personopplysningene vernes mot risikoen for misbruk på en effektiv måte([183]). Lovgivningen skal særlig angi under hvilke omstendigheter og på hvilke vilkår et tiltak for behandling av slike opplysninger kan vedtas([184]), og stille krav til uavhengig tilsyn med at disse kravene oppfylles([185]).

143) For det tredje skal denne lovgivningen og kravene i den være rettslig bindende i henhold til nasjonal rett. Dette gjelder først og fremst alle myndighetene i det aktuelle tredjelandet, men disse rettslige kravene skal også kunne rettshåndheves overfor disse myndighetene([186]). Registrerte skal særlig ha mulighet til å bringe en sak inn for en uavhengig og upartisk domstol for å få innsyn i egne personopplysninger eller for å få disse opplysningene rettet eller slettet([187]).

3.1 Generell rettslig ramme

144) Begrensningene og garantiene som gjelder for sørkoreanske offentlige myndigheters innsamling og etterfølgende bruk av personopplysninger, følger av den overordnede forfatningsmessige rammen, spesifikke lover som regulerer deres aktiviteter på området strafferettslig håndheving og nasjonal sikkerhet, og reglene som spesifikt gjelder for behandling av personopplysninger.

([181]) Som forklart i betraktning 127 kan feil bruk av opplysninger utgjøre en straffbar handling i henhold til straffeloven.

([182]) Se *Schrems II* nr. 174–175 og angitt rettspraksis. Når det gjelder tilgang for medlemsstatenes offentlige myndigheter, se også sak C-623/17 Privacy International, ECLI:EU:C:2020:790 nr. 65, og forente saker C-511/18, C-512/18 og C-520/18 La Quadrature du Net and Others, ECLI:EU:C:2020:791 nr. 175.

([183]) Se Schrems II nr. 176 og 181 og angitt rettspraksis. Når det gjelder tilgang for medlemsstatenes offentlige myndigheter, se også Privacy International nr. 68 og *La Quadrature du Net and Others* nr. 132.

([184]) Se *Schrems II* nr. 176. Når det gjelder tilgang for medlemsstatenes offentlige myndigheter, se også Privacy International nr. 68 og *La Quadrature du Net and Others* nr. 132.

([185]) Se *Schrems II* nr. 179.

([186]) Se *Schrems II* nr. 181–182.

([187]) Se *Schrems I* nr. 95 og *Schrems II* nr. 194. I den forbindelse har Den europeiske unions domstol særlig understreket at overholdelse av artikkel 47 i Den europeiske unions pakt om grunnleggende rettigheter som sikrer retten til et effektivt rettsmiddel ved en uavhengig og upartisk domstol — «bidrar til det beskyttelsesnivået som kreves i Den europeiske union [og] skal fastsettes av Kommisjonen før den treffer en beslutning om tilstrekkelig beskyttelsesnivå i henhold til artikkel 45 nr. 1 i forordning (EU) 2016/679» (*Schrems II* nr. 186).

145) For det første er sørkoreanske offentlige myndigheters tilgang til personopplysninger underlagt de generelle prinsippene om lovlighet, nødvendighet og forholdsmessighet som følger av den sørkoreanske forfatningen([188]). Grunnleggende rettigheter og friheter (herunder retten til personvern og retten til personvern i forbindelse med korrespondanse)([189]) kan bare begrenses ved lov og når det er nødvendig av hensyn til den nasjonale sikkerheten eller for å opprettholde lov og orden med henblikk på borgernes velferd. Slike begrensninger må ikke påvirke det vesentlige innholdet i den aktuelle rettigheten eller friheten. Når det gjelder ransaking og beslaglegging, er det spesifikt fastsatt i forfatningen at dette bare kan skje som fastsatt i loven, på grunnlag av en kjennelse utstedt av en dommer og ved å overholde prinsippet om en rettferdig rettergang([190]). Enkeltpersoner kan også påberope seg sine rettigheter og friheter ved forfatningsdomstolen dersom de mener at de er blitt krenket av offentlige myndigheters utøvelse av myndighet([191]). På samme måte har personer som har lidd skade som følge av en ulovlig handling begått av en offentlig tjenestemann i forbindelse med vedkommendes utøvelse av sine offisielle funksjoner, rett til å kreve en rimelig erstatning([192]).

146) For det andre, som beskrevet nærmere i avsnitt 3.2.1 og 3.3.1, gjenspeiles de generelle prinsippene nevnt i betraktning 145 i de spesifikke lovene som regulerer rettshåndhevende myndigheters og nasjonale sikkerhetsmyndigheters myndighet. Når det gjelder strafferettslig etterforskning er det i straffeprosessloven (Criminal Procedure Act – CPA) fastsatt at tvangstiltak bare kan treffes dersom det er uttrykkelig fastsatt i CPA, og i så lite omfang som nødvendig for å oppfylle formålet med etterforskningen([193]). På samme måte forbyr artikkel 3 i loven om personvern i forbindelse med kommunikasjon (Communications Privacy Protection Act – CPPA) tilgang til privat kommunikasjon, unntatt på grunnlag av loven og med forbehold for begrensningene og garantiene fastsatt der. På området nasjonal sikkerhet er det i loven om den nasjonale etterretningstjenesten (National Intelligence Service Act – NIS-loven) fastsatt at enhver tilgang til kommunikasjons- eller lokaliseringsopplysninger må være i samsvar med loven, og at misbruk av myndighet og overtredelser av loven omfattes av strafferettslige sanksjoner([194]).

147) For det tredje omfattes offentlige myndigheters behandling av personopplysninger, herunder for formål knyttet til rettshåndheving og nasjonal sikkerhet, av reglene for vern av personopplysninger fastsatt i PIPA([195]). Som et generelt prinsipp skal offentlige myndigheter i henhold til artikkel 5 nr. 1 i PIPA utarbeide strategier for å hindre «misbruk og feil bruk av personopplysninger, gjennomgripende overvåking og sporing osv. og for å styrke menneskers verdighet og personvern». I tillegg må alle behandlingsansvarlige behandle personopplysninger på en måte som minimerer risikoen for å krenke den registrertes personvern (artikkel 3 nr. 6 i PIPA).

148) Alle kravene i PIPA, som er nærmere beskrevet i avsnitt 2, gjelder behandling av personopplysninger for rettshåndhevende formål. Dette omfatter de sentrale prinsippene (f.eks. om lovlig og rettferdig behandling, formålsbegrensning, riktighet, dataminimering, lagringsbegrensning, sikkerhet og åpenhet), forpliktelsene (f.eks. med hensyn til underretning om brudd på opplysningssikkerheten og sensitive opplysninger) og rettighetene (innsyn, retting, sletting og innstilling av behandlingen).

149) Selv om behandling av personopplysninger for formål knyttet til nasjonal sikkerhet omfattes av et mer begrenset sett av bestemmelser i henhold til PIPA, får de sentrale prinsippene samt reglene for tilsyn, håndheving og klageadgang anvendelse([196]). I artikkel 3 og 4 i PIPA fastsettes mer spesifikt de generelle prinsippene for vern av personopplysninger (lovlig og rettferdig behandling, formålsbegrensning, riktighet, dataminimering, sikkerhet og åpenhet) og individuelle rettigheter (retten til å bli underrettet, retten til innsyn og retten til retting og sletting og til å få behandlingen innstilt)([197]). I artikkel 4 nr. 5 i PIPA er det dessuten fastsatt at enkeltpersoner ved hjelp av en rask og rettferdig prosedyre har rett til egnet erstatning for skader som oppstår som følge av behandlingen av deres personopplysninger.

([188]) Se vedlegg II avsnitt 1.1.

([189]) Artikkel 37 nr. 2 i forfatningen.

([190]) Artikkel 16 og 12 nr. 3 i forfatningen. I artikkel 12 nr. 3 i forfatningen er det fastsatt under hvilke ekstraordinære omstendigheter det kan foretas ransaking eller beslaglegging uten kjennelse (selv om det fremdeles kreves en kjennelse i ettertid), det vil si i *in flagranti*-situasjoner eller ved straffbare forhold som fører til fengsel i minst tre år, dersom det er en risiko for at bevismateriale vil bli ødelagt, eller for at den mistenkte unnslipper.

([191]) Artikkel 68 nr. 1 i loven om forfatningsdomstolen.

([192]) Artikkel 29 nr. 1 i forfatningen.

([193]) Artikkel 199 nr. 1 i CPA. Mer generelt skal offentlige myndigheter når de utøver sin myndighet i henhold til CPA, respektere de mistenktes og andre berørte personers grunnleggende rettigheter (artikkel 198 nr. 2 i CPA).

([194]) Artikkel 14 i NIS-loven.

([195]) Se vedlegg II avsnitt 1.2.

([196]) Artikkel 58 nr. 1 pkt. 2 i PIPA. Se også melding 2021-5 avsnitt 6 (vedlegg I). Dette unntaket fra visse bestemmelser i PIPA gjelder bare når personopplysninger behandles «for formål knyttet til nasjonal sikkerhet». Når den nasjonale sikkerhetssituasjonen som er årsaken til at personopplysningene behandles, ikke lenger foreligger, er det ikke lenger mulig å gjøre bruk av unntaket, og alle bestemmelsene i PIPA får anvendelse.

([197]) Slike rettigheter kan bare begrenses dersom det er fastsatt ved lov, i den grad og så lenge det er nødvendig og forholdsmessig for å beskytte et viktig mål av allmenn interesse, eller dersom det å gi rettigheten kan skade en tredjeparts liv eller legeme eller utgjør en uberettiget krenking av en tredjeparts eiendom og andre interesser. Se melding 2021-5 avsnitt 6.

Dette utfylles av mer spesifikke forpliktelser til bare å behandle personopplysninger i så lite omfang som nødvendig for å oppfylle det tiltenkte formålet, og i kortest mulig tid, til å treffe nødvendige tiltak for å sikre en sikker håndtering av opplysningene og egnet behandling (for eksempel tekniske, organisatoriske og fysiske garantier) og til å treffe tiltak for egnet behandling av individuelle klager)([198]). For det fjerde får de generelle prinsippene om lovlighet, nødvendighet og forholdsmessighet i den sørkoreanske forfatningen (se betraktning 145) også anvendelse på behandling av personopplysninger for formål knyttet til nasjonal sikkerhet.

150) Enkeltpersoner kan påberope seg disse generelle begrensningene og garantiene ved uavhengige tilsynsorganer (f.eks. kommisjonen for vern av personopplysninger og/eller den nasjonale menneskerettighetskommisjonen, se betraktning 177–178) og domstoler (se betraktning 179–183) for å få prøvet sin sak.

3.2 Sørkoreanske offentlige myndigheters tilgang til og bruk av personopplysninger for formål knyttet til strafferettslig håndheving

151) Ved Republikken Koreas lovgivning pålegges det en rekke begrensninger av tilgangen til og bruken av personopplysninger for formål knyttet til strafferettslig håndheving, og den inneholder en rekke tilsyns- og prøvingsmekanismer som er i samsvar med kravene nevnt i betraktning 141–143 i denne beslutningen. Vilkårene for slik tilgang og garantiene som gjelder for utøvelsen av denne myndigheten, beskrives nærmere i avsnittene nedenfor.

3.2.1 *Rettslig grunnlag, begrensninger og garantier*

152) Personopplysninger som behandles av sørkoreanske behandlingsansvarlige, og som vil bli overført fra Unionen i henhold til denne beslutningen([199]), kan samles inn av sørkoreanske myndigheter for formål knyttet til strafferettslig håndheving i forbindelse med ransaking eller beslaglegging (på grunnlag av CPA), gjennom tilgang til kommunikasjonsopplysninger (på grunnlag av CPPA) eller ved innhenting av abonnentopplysninger på grunnlag av anmodninger om frivillig utlevering (på grunnlag av loven om telekommunikasjonsvirksomhet (Telecommunications Business Act – TBA)([200]).

3.2.1.1 Ransaking og beslaglegging

153) I henhold til CPA kan ransaking eller beslaglegging bare skje dersom en person er mistenkt for et straffbart forhold og det er nødvendig for etterforskningen, og det er etablert en forbindelse mellom etterforskningen og personen som skal ransakes, eller gjenstanden som skal kontrolleres eller beslaglegges([201]). Dessuten kan ransaking eller beslaglegging (som alle tvangstiltak) bare godkjennes/gjennomføres i den grad det er strengt nødvendig([202]). Dersom en ransaking gjelder en diskett eller et annet datalagringsmedium, er det i prinsippet bare de nødvendige opplysningene (kopiert eller skrevet ut) som vil bli beslaglagt, og ikke hele mediet([203]). Mediet kan bare beslaglegges dersom det anses som praktisk umulig å skrive ut eller kopiere de aktuelle opplysningene separat eller å oppfylle formålet med ransakingen på annen måte([204]). CPA fastsetter derfor klare og presise regler for omfanget og anvendelsen av disse tiltakene, noe som sikrer at inngripenen i enkeltpersoners rettigheter i forbindelse med en ransaking eller beslaglegging begrenses til det som er nødvendig for en spesifikk strafferettslig etterforskning, og står i rimelig forhold til formålet som søkes oppnådd.

([198]) Artikkel 58 nr. 4 i PIPA.

([199]) Se vedlegg II avsnitt 2.1. I den sørkoreanske regjeringens offisielle redegjørelse (vedlegg II avsnitt 2.1) vises det også til muligheten for å samle inn opplysninger om finansielle transaksjoner med henblikk på å forebygge hvitvasking av penger og finansiering av terrorisme på grunnlag av loven om rapportering og bruk av spesifikke opplysninger om finansielle transaksjoner (Act on Reporting and Using Specified Financial Transaction Information – ARUSFTI). I henhold til ARUSFTI er det imidlertid bare behandlingsansvarlige som behandler personlige kredittopplysninger i henhold til CIA og som er underlagt FSCs tilsyn, som pålegges en utleveringsplikt (se betraktning 13). Ettersom behandling av personlige kredittopplysninger som utføres av slike behandlingsansvarlige, ikke omfattes av denne beslutningens virkeområde, er ARUSFTI ikke relevant for denne vurderingen.

([200]) Artikkel 3 i CPPA nevner også loven om militærdomstolen som et mulig rettslig grunnlag for innsamling av kommunikasjonsopplysninger. Den loven regulerer imidlertid innsamling av opplysninger om militært personell og kan bare anvendes på sivile i et begrenset antall tilfeller (dersom militært personell og sivile begår en straffbar handling sammen, eller dersom en person begår en straffbar handling mot militæret, kan det for eksempel anlegges sak ved en militærdomstol, se artikkel 2 i loven om militærdomstolen). Loven inneholder generelle bestemmelser om ransaking og beslaglegging som svarer til bestemmelsene i CPA (se for eksempel artikkel 146–149 og 153–156 i loven om militærdomstolen), og for eksempel om at postforsendelser bare kan samles inn når det er nødvendig i forbindelse med en etterforskning, og på grunnlag av en kjennelse fra militærdomstolen. I den grad elektronisk kommunikasjon samles inn på grunnlag av denne loven, får begrensningene og garantiene i CPPA anvendelse. Se vedlegg II avsnitt 2.2.2 og fotnote 50.

([201]) Artikkel 215 nr. 1 og 2 i CPA. Se også artikkel 106 nr. 1 og artikkel 107 og 109 i CPA, der det er fastsatt at domstoler kan gjennomføre ransaking og beslaglegging så lenge de berørte gjenstandene eller personene anses for å ha tilknytning til en bestemt sak. Se vedlegg II avsnitt 2.2.1.2.

([202]) Artikkel 199 nr. 1 i CPA.

([203]) Artikkel 106 nr. 3 i CPA.

([204]) Artikkel 106 nr. 3 i CPA.

154) Når det gjelder prosessuelle garantier, skal det i henhold til CPA innhentes en rettskjennelse for å kunne gjennomføre en ransaking eller beslaglegging([205]). Ransaking eller beslaglegging uten kjennelse er bare tillatt i unntakstilfeller, det vil si i hastetilfeller([206]), på stedet i forbindelse med at en mistenkt pågripes eller holdes i varetekt([207]), eller dersom en gjenstand kastes eller utleveres frivillig av en mistenkt eller en tredjeperson (av den berørte personen selv når det gjelder personopplysninger([208]). Ulovlig ransaking og beslaglegging er underlagt strafferettslige sanksjoner([209]), og bevismateriale innhentet i strid med CPA godtas ikke([210]). De berørte personene skal alltid uten opphold underrettes om en ransaking eller beslaglegging (herunder beslaglegging av deres opplysninger)([211]), noe som vil lette utøvelsen av deres materielle rettigheter og retten til prøving (se særlig muligheten til å bestride iverksettingen av en kjennelse om beslaglegging, se betraktning 180).

3.2.1.2 Tilgang til kommunikasjonsopplysninger

155) På grunnlag av CPPA kan sørkoreanske strafferettshåndhevende myndigheter treffe to typer tiltak([212]): For det første innsamling av «kommunikasjonsbekreftelsesdata»([213]), som omfatter datoen og start- og sluttidspunktet for telekommunikasjoner, antall utgående og innkommende samtaler samt den andre partens abonnentnummer, bruksfrekvens, loggfiler om bruken av telekommunikasjonstjenester og lokaliseringsopplysninger (for eksempel fra signalmaster der signaler mottas), og for det andre «kommunikasjonsbegrensende tiltak», som omfatter både innsamling av innholdet i tradisjonell post og direkte avlytting av innhold i telekommunikasjon([214]).

156) Tilgang til kommunikasjonsbekreftelsesdata tillates bare når det er nødvendig for å gjennomføre en strafferettslig etterforskning eller iverksette en dom([215]), og på grunnlag av en rettskjennelse([216]). I denne forbindelse skal det i henhold til CPPA gis detaljerte opplysninger både i begjæringen om kjennelsen (for eksempel om begrunnelsen for begjæringen, forholdet mellom den aktuelle personen/abonnenten og de nødvendige opplysningene) og i selve kjennelsen (for eksempel om tiltakets formål, mål og omfang)([217]). Innsamling uten kjennelse kan bare finne sted når

([205]) Artikkel 215 nr. 1 og 2 og artikkel 113 i CPA. Når det framsettes en begjæring om kjennelse, skal den berørte myndigheten framlegge dokumentasjon som viser hvorfor en person mistenkes for å ha begått en straffbar handling, at ransakingen, inspeksjonen eller beslagleggingen er nødvendig, og at de relevante gjenstandene som skal beslaglegges, finnes (artikkel 108 nr. 1 i straffeprosessforordningen). Selve kjennelsen skal blant annet inneholde navnet på den mistenkte og en beskrivelse av den straffbare handlingen, stedet, personen eller gjenstandene som skal ransakes, eller gjenstandene som skal beslaglegges, utstedelsesdatoen og den faktiske anvendelsesperioden (artikkel 114 nr. 1 sammenholdt med artikkel 219 i CPA). Se vedlegg II avsnitt 2.2.1.2.

([206]) Når det er ikke er mulig å innhente en kjennelse fordi situasjonen på gjerningsstedet gjør at det ikke er tid til det (artikkel 216 nr. 3 i CPA), skal det uten opphold innhentes en kjennelse i ettertid (artikkel 216 nr. 3 i CPA).

([207]) Artikkel 216 nr. 1 og 2 i CPA.

([208]) Artikkel 218 i CPA. Som forklart i vedlegg II avsnitt 2.2.1.2 godtas frivillig utleverte gjenstander dessuten som bevismateriale i rettssaker bare dersom det ikke er noen rimelig tvil om at utleveringen er frivillig, noe det er opp til påtalemyndigheten å bevise.

([209]) Artikkel 321 i straffeloven.

([210]) Artikkel 308-2 i CPA. En person (og vedkommendes advokat) kan dessuten være til stede når en kjennelse om ransaking eller beslaglegging iverksettes, og kan derfor også gjøre innvendinger på iverksettingstidspunktet (artikkel 121 og 219 i CPA).

([211]) Artikkel 121 og 122 i CPA (når det gjelder ransaking) og artikkel 219 sammenholdt med artikkel 106 nr. 4 i CPA (når det gjelder beslaglegging).

([212]) Se også vedlegg II avsnitt 2.2.2.1. Slike tiltak kan treffes med tvungen bistand fra teleoperatører på grunnlag av en skriftlig tillatelse fra en domstol (artikkel 9 nr. 2 i CPPA), som gis til og skal oppbevares av operatørene (artikkel 15-2 i CPPA og artikkel 12 i gjennomføringsdekretet til CPPA). Telekommunikasjonsleverandører kan nekte å samarbeide dersom opplysningene om den aktuelle personen angitt i domstolens skriftlige tillatelse (f.eks. personens telefonnummer) er uriktige, og det er under alle omstendigheter forbudt å utlevere passord som brukes i forbindelse med telekommunikasjon (artikkel 9 nr. 4 i CPPA).

([213]) Artikkel 2 nr. 11 i CPPA.

([214]) Se artikkel 2 nr. 6 i CPPA der det vises til «sensur» (åpning av post uten den berørte partens samtykke eller innsamling av kunnskap om eller registrering eller tilbakeholding av innhold på annen måte), og artikkel 2 nr. 7 i CPPA der det vises til «avlytting» (innsamling eller registrering av innholdet i telekommunikasjon ved å lytte til eller kollektivt fortolke lyder, ord, symboler eller bilder i kommunikasjonen ved bruk av elektronisk og mekanisk utstyr uten den berørte partens samtykke, eller forstyrre overføringen og mottaket av den).

([215]) Artikkel 13 nr. 1 i CPPA. Se også vedlegg II avsnitt 2.2.2.3. Dessuten kan lokaliseringsdata i sanntid og kommunikasjonsbekreftelsesdata som gjelder en bestemt basestasjon, bare samles inn med henblikk på etterforskning av alvorlige straffbare forhold eller dersom det ellers ville vært vanskelig å hindre et straffbart forhold eller samle inn bevismateriale (artikkel 13 nr. 2 i CPPA). Dette gjenspeiler behovet for å innføre ytterligere garantier ved spesielt personverninngripende tiltak i tråd med forholdsmessighetsprinsippet.

([216]) Artikkel 13 og 6 i CPPA.

([217]) Se artikkel 13 nr. 3 og 9 sammenholdt med artikkel 6 nr. 4 og 6 i CPPA.

saken haster og dette gjør at det ikke er mulig å innhente en rettskjennelse, i så fall skal kjennelsen innhentes og framlegges for telekommunikasjonsleverandøren umiddelbart etter at det er anmodet om opplysningene([218]). Dersom retten avslår å gi en tillatelse i etterkant, skal de innsamlede opplysningene tilintetgjøres([219]).

157) Når det gjelder ytterligere garantier med hensyn til innsamling av kommunikasjonsbekreftelsesdata, stilles det i CPPA særlige krav til registrering og åpenhet([220]). Både strafferettshåndhevende myndigheter ([221]) og telekommunikasjonsleverandører([222]) skal føre registre over anmodninger og utleveringer som er gjort. I tillegg skal strafferettshåndhevende myndigheter i prinsippet underrette de berørte personene om at deres kommunikasjonsbekreftelsesdata er blitt samlet inn([223]). En slik underretning kan bare utsettes i unntakstilfeller på grunnlag av en tillatelse fra lederen for et kompetent lokalt statsadvokatkontor([224]). En slik tillatelse kan bare gis dersom det er sannsynlig at underretningen vil 1) sette den nasjonale sikkerheten og den offentlige sikkerheten og ordenen i fare, 2) forårsake død eller kroppsskade, 3) hindre en rettferdig rettergang (for eksempel føre til ødeleggelse av bevismateriale eller trusler mot vitner) eller 4) ærekrenke den mistenkte, ofrene eller andre personer med tilknytning til saken eller krenke deres personvern. I slike tilfeller skal underretningen gis senest 30 dager etter at grunnene til utsettelsen ikke lenger foreligger([225]). Etter underretningen har de berørte personene rett til å få informasjon om hvorfor deres opplysninger er blitt samlet inn([226]).

158) Det gjelder strengere regler for kommunikasjonsbegrensende tiltak, som bare må brukes når det er vektige grunner til å mistenke at visse alvorlige straffbare handlinger som er spesifikt oppført i CPPA, planlegges, begås eller er blitt begått([227]). Kommunikasjonsbegrensende tiltak kan dessuten bare treffes som en siste utvei og dersom det er vanskelig å hindre at det begås en straffbar handling, pågripe en forbryter eller samle inn bevismateriale på annen måte([228]). De skal opphøre umiddelbart når de ikke lenger er nødvendige, for å sikre at krenkingen av personvernet i forbindelse med kommunikasjon er så begrenset som mulig([229]). Opplysninger som er innhentet på ulovlig vis ved bruk av kommunikasjonsbegrensende tiltak, godtas ikke som bevismateriale i rettssaker eller disiplinærsaker([230]).

159) Når det gjelder prosessuelle garantier, skal det i henhold til CPPA innhentes en rettskjennelse for å gjennomføre kommunikasjonsbegrensende tiltak([231]). I henhold til CPPA skal begjæringen om kjennelse og selve kjennelsen inneholde detaljerte opplysninger([232]), herunder om begrunnelsen for begjæringen og kommunikasjonen som skal samles inn (som må tilhøre den mistenkte personen som er gjenstand for etterforskningen)([233]). Slike tiltak kan bare treffes uten kjennelse dersom det foreligger en overhengende fare for organisert kriminalitet eller andre alvorlige straffbare forhold som direkte kan forårsake dødsfall eller alvorlig skade, og dersom det foreligger en nødssituasjon

([218]) Artikkel 13 nr. 2 i CPPA.
([219]) Artikkel 13 nr. 3 i CPPA.
([220]) Se vedlegg II avsnitt 2.2.2.3.
([221]) Artikkel 13 nr. 5 og 6 i CPPA.
([222]) Artikkel 13 nr. 7 i CPPA. Telekommunikasjonsleverandører må dessuten avlegge rapport for departementet for vitenskap og IKT om utleveringen av kommunikasjonsbekreftelsesdata to ganger i året.
([223]) Se artikkel 13-3 nr. 7 sammenholdt med artikkel 9-2 i CPPA. Enkeltpersoner må underrettes senest 30 dager etter at det er truffet beslutning om å (ikke) reise tiltale, eller senest 30 dager og ett år etter at det er truffet beslutning om å midlertidig oppheve en tiltale (selv om underretningen under alle omstendigheter skal skje senest ett år og 30 dager etter at opplysningene er samlet inn), se artikkel 13-3 nr. 1 i CPPA.
([224]) Artikkel 13-3 nr. 2–3 i CPPA.
([225]) Artikkel 13-3 nr. 4 i CPPA.
([226]) Artikkel 13-3 nr. 5 i CPPA. På anmodning fra den aktuelle personen skal påtalemyndigheten eller kriminalpolitiet gi en skriftlig begrunnelse senest 30 dager etter å ha mottatt anmodningen, med mindre et av unntakene for å utsette underretningen får anvendelse (artikkel 13-3 nr. 6 i CPPA).
([227]) For eksempel opprør, narkotikarelaterte straffbare handlinger, straffbare handlinger der eksplosiver er involvert, og straffbare handlinger knyttet til nasjonal sikkerhet, diplomatiske forbindelser eller militærbaser og -installasjoner, se artikkel 5 nr. 1 i CPPA. Se også vedlegg II avsnitt 2.2.2.2.
([228]) Artikkel 3 nr. 2 og artikkel 5 nr. 1 i CPPA.
([229]) Artikkel 2 i gjennomføringsdekretet til CPPA.
([230]) Artikkel 4 i CPPA.
([231]) Artikkel 6 nr. 1–2 og 5–6 i CPPA.
([232]) En begjæring om kjennelse skal inneholde en beskrivelse av 1) de vektige grunnene (*prima facie*) til å mistenke at en av de oppførte straffbare handlingen planlegges, begås eller er begått, samt eventuell dokumentasjon, 2) de kommunikasjonsbegrensende tiltakene og tiltakenes mål, omfang, formål og varighet og 3) stedet der tiltakene vil bli gjennomført, og hvordan de vil bli gjennomført (artikkel 6 nr. 4 i CPPA og artikkel 4 nr. 1 i gjennomføringsdekretet til CPPA). I selve kjennelsen angis tiltakene og tiltakenes mål, omfang, varighet, stedet der de vil bli gjennomført, og hvordan de vil bli gjennomført (artikkel 6 nr. 6 i CPPA).
([233]) Et kommunikasjonsbegrensende tiltak må være rettet mot spesifikke postforsendelser eller spesifikk telekommunikasjon som sendes eller mottas av den mistenkte, eller postforsendelser eller telekommunikasjon som sendes eller mottas av den mistenkte i en bestemt periode (artikkel 5 nr. 2 i CPPA).

som gjør det umulig å følge den vanlige prosedyren([234]). Da skal det imidlertid framsettes en begjæring om kjennelse umiddelbart etter at tiltaket er truffet([235]). Kommunikasjonsbegrensende tiltak kan bare gjennomføres i en periode på høyst to måneder([236]) og kan bare forlenges med rettens godkjenning dersom vilkårene for å gjennomføre tiltakene fremdeles er oppfylt([237]). Den forlengede perioden kan ikke være lenger enn ett år eller tre år for visse spesielt alvorlige straffbare handlinger (som for eksempel er knyttet til opprør, aggresjon utenfra, nasjonal sikkerhet)([238]).

160) Som ved innsamling av kommunikasjonsbekreftelsesdata kreves det i henhold til CPPA at telekommunikasjonsleverandører([239]) og rettshåndhevende myndigheter([240]) skal føre registre over gjennomføringen av de kommunikasjonsbegrensende tiltakene, og loven inneholder bestemmelser om underretning av den aktuelle personen, som i unntakstilfeller kan utsettes dersom det er nødvendig av hensyn til viktige allmenne interesser([241]).

161) Manglende overholdelse av flere av begrensningene og garantiene i CPPA (herunder for eksempel forpliktelsen til å innhente en kjennelse, føre registre og underrette den berørte personen), både når det gjelder innsamling av kommunikasjonsbekreftelsesdata og bruken av kommunikasjonsbegrensende tiltak, er gjenstand for strafferettslige sanksjoner([242]).

162) Strafferettshåndhevende myndigheters myndighet til å samle inn kommunikasjonsopplysninger på grunnlag av CPPA (både kommunikasjonsinnhold og kommunikasjonsbekreftelsesdata) er derfor begrenset av klare og presise regler og underlagt en rekke garantier. Disse garantiene sikrer særlig tilsyn med gjennomføringen av slike tiltak, både på forhånd (gjennom rettslig forhåndsgodkjenning) og i ettertid (gjennom krav til dokumentasjon og rapportering) og letter enkeltpersoners tilgang til effektive rettsmidler (ved å sikre at de informeres om at deres opplysninger samles inn).

3.2.1.3 Anmodninger om frivillig utlevering av abonnentopplysninger

163) I tillegg til å basere seg på tvangstiltakene beskrevet i betraktning 153–162 kan sørkoreanske rettshåndhevende myndigheter be telekommunikasjonsleverandører om frivillig utlevering av «kommunikasjonsopplysninger» til støtte for en straffesak, etterforskning eller iverksetting av en dom (artikkel 83 nr. 3 i TBA). Denne muligheten finnes bare for begrensede datasett, det vil si brukernes navn, folkeregisternummer, adresse og telefonnummer, datoene for brukernes tegning eller oppsigelse av abonnement og brukeridentifikasjonskoder (det vil si koder som brukes for å identifisere den rettmessige brukeren av datasystemer eller kommunikasjonsnettverk)([243]). Ettersom det bare er enkeltpersoner som inngår avtaler om tjenester direkte med en sørkoreansk telekommunikasjonsleverandør, som anses som «brukere»([244]), omfattes EU-borgere som har fått sine opplysninger overført til Republikken Korea, normalt ikke av denne kategorien([245]).

164) Det gjelder forskjellige begrensninger for en slik frivillig utlevering, både for den rettshåndhevende myndighetens utøvelse av myndighet og for teleoperatørens respons. Som et generelt krav skal de rettshåndhevende myndighetene handle i samsvar med de forfatningsmessige prinsippene om nødvendighet og forholdsmessighet (artikkel 12 nr. 1 og artikkel 37 nr. 2 i forfatningen), herunder når de anmoder om informasjon på frivillig grunnlag. De skal i tillegg overholde PIPA, særlig ved bare å samle inn personopplysninger i det omfang som er nødvendig for å oppfylle et

([234]) Artikkel 8 nr. 1 i CPPA. Innsamling av opplysninger i nødssituasjoner må imidlertid alltid skje i samsvar med en «erklæring om sensur/avlytting i nødssituasjoner», og myndigheten som foretar innsamlingen, må føre et register over eventuelle hastetiltak (artikkel 8 nr. 4 i CPPA).

([235]) Innsamlingen må innstilles umiddelbart dersom den rettshåndhevende myndigheten ikke oppnår tillatelse fra en domstol innen 36 timer (artikkel 8 nr. 2 i CPPA), i så fall skal de innsamlede opplysningene tilintetgjøres, som forklart i vedlegg II avsnitt 2.2.2.2. Domstolen må også underrettes dersom hastetiltakene er blitt avsluttet så raskt at det ikke er behov for tillatelse (for eksempel dersom den mistenkte arresteres umiddelbart etter at avlyttingen har startet, se artikkel 8 nr. 5 i CPPA). Da må domstolen gis opplysninger om formålet, målet, omfanget, varigheten, gjennomføringsstedet og innsamlingsmetoden samt grunnene til at det ikke er inngitt en anmodning om domstolstillatelse (artikkel 8 nr. 6–7 i CPPA).

([236]) Artikkel 6 nr. 7 i CPPA. Dersom formålet med tiltakene oppnås før denne fristen, skal tiltakene innstilles umiddelbart.

([237]) Artikkel 6 nr. 7–8 i CPPA.

([238]) Artikkel 6 nr. 8 i CPPA.

([239]) Artikkel 9 nr. 3 i CPPA.

([240]) Artikkel 18 nr. 1 i gjennomføringsdekretet til CPPA.

([241]) Påtalemyndigheten må underrette den aktuelle personen senest 30 dager etter at det er reist tiltale eller besluttet å ikke reise tiltale eller foreta pågripelse (artikkel 9-2 nr. 1 i CPPA). Underretningen kan utsettes med godkjenning fra lederen for det lokale statsadvokatkontoret dersom det er sannsynlig at den vil bringe den nasjonale sikkerheten i alvorlig fare eller forstyrre den offentlige sikkerheten og ordenen, eller dersom det er sannsynlig at den vil påføre andres liv og legeme vesentlig skade (artikkel 9-2 nr. 4–6 i CPPA).

([242]) Artikkel 16 og 17 i CPPA.

([243]) Artikkel 83 nr. 3 i TBA. Se også vedlegg II avsnitt 2.2.3.

([244]) Artikkel 2 nr. 9 i TBA.

([245]) Se også vedlegg II avsnitt 2.2.3.

berettiget formål, og på en måte som har så få innvirkninger som mulig på den enkeltes personvern (for eksempel artikkel 3 nr. 1 og 6 i PIPA). Nærmere bestemt skal anmodninger om innhenting av kommunikasjonsopplysninger på grunnlag av TBA inngis skriftlig med en angivelse av begrunnelsen for anmodningen, lenken til den relevante brukeren og omfanget av opplysningene det bes om([246]).

165) Telekommunikasjonsleverandører plikter ikke å etterkomme slike anmodninger og kan bare gjøre det i samsvar med PIPA. Dette betyr særlig at de må foreta en avveining mellom de forskjellige interessene som står på spill, og at de ikke kan videreformidle opplysningene dersom det er sannsynlig at det vil krenke en enkeltpersons eller en tredjeparts interesser urettmessig([247]). Dette vil for eksempel være tilfellet dersom det er klart at den anmodende myndigheten har misbrukt sin myndighet([248]). Teleoperatører må føre registre over opplysninger som utleveres i henhold til TBA, og to ganger i året avlegge rapport for ministeren for vitenskap og IKT([249]).

166) I samsvar med melding 2021-5 avsnitt 3 (vedlegg I) må telekommunikasjonsleverandører, når de frivillig etterkommer en anmodning, dessuten i prinsippet underrette den berørte personen([250]). Dette gjør det mulig for den berørte personen å utøve sine rettigheter og, dersom vedkommendes opplysninger er blitt utlevert på ulovlig vis, å inngi en klage enten på den behandlingsansvarlige (for eksempel for å ha utlevert opplysningene i strid med PIPA eller for å ha etterkommet en anmodning som helt klart var uforholdsmessig) eller på den rettshåndhevende myndigheten (for eksempel for å ha gått ut over det som er nødvendig og forholdsmessig, eller for ikke å ha respektert de prosessuelle kravene i TBA).

3.2.2 *Videre bruk av de innsamlede opplysningene*

167) Behandlingen av personopplysninger som samles inn av sørkoreanske strafferettshåndhevende myndigheter, skal oppfylle alle kravene i PIPA, herunder når det gjelder formålsbegrensning (artikkel 3 nr. 1–2 i PIPA), lovlig bruk og videreformidling til tredjeparter (artikkel 15, 17 og 18 i PIPA), internasjonale overføringer (artikkel 17 og 18 i PIPA sammenholdt med melding 2021-5) avsnitt 2([251]), forholdsmessighet/dataminimering (artikkel 3 nr. 1 og 6 i PIPA) og lagringsbegrensning (artikkel 21 i PIPA)([252]).

168) Når det gjelder kommunikasjonsinnhold som oppnås gjennom kommunikasjonsbegrensende tiltak, begrenser CPPA spesifikt den mulige bruken av slikt innhold til etterforskning, rettsforfølgning eller hindring av alvorlige straffbare forhold([253]), disiplinærsaker i forbindelse med disse straffbare forholdene, i forbindelse med erstatningskrav reist av en part i kommunikasjonen eller dersom dette er spesifikt tillatt i henhold til annen lovgivning([254]). Innsamlet innhold i telekommunikasjon som overføres via internett, kan dessuten bare lagres med godkjenning fra den domstolen som godkjente de kommunikasjonsbegrensende tiltakene([255]), for det formålet å bruke det i forbindelse med etterforskning, rettsforfølgning eller forebygging av alvorlige straffbare forhold([256]). Mer generelt forbyr CPPA utlevering av konfidensielle opplysninger som er innhentet ved hjelp av kommunikasjonsbegrensende tiltak, og bruk av slike opplysninger for å skade omdømmet til de som var omfattet av tiltakene([257]).

3.2.3 *Tilsyn*

169) Republikken Korea har forskjellige organer som fører tilsyn med de strafferettshåndhevende myndighetenes aktiviteter([258]).

([246]) Artikkel 83 nr. 4 i TBA. Dersom saken haster og det derfor ikke er mulig å inngi en skriftlig anmodning, skal den skriftlige anmodningen inngis så snart årsaken til at saken haster, ikke lenger foreligger (artikkel 83 nr. 4 i TBA).

([247]) Artikkel 18 nr. 2 i PIPA.

([248]) Høyesteretts avgjørelse 2012Da105482 av 10. mars 2016. Se også vedlegg II avsnitt 2.2.3 om denne høyesterettsavgjørelsen.

([249]) Artikkel 83 nr. 5–6 i TBA.

([250]) For dette kravet gjelder det begrensede og kvalifiserte unntak, særlig dersom og så lenge underretningen vil kunne bringe en pågående strafferettslig etterforskning i fare eller det er sannsynlig at det vil skade en annen persons liv eller legeme, dersom disse rettighetene eller interessene klart går foran den registrertes rettigheter. Se avsnitt 3 punkt iii) nr. 1 i meldingen.

([251]) Sørkoreanske offentlige myndigheter skal gjennom et rettslig bindende instrument sikre et beskyttelsesnivå som svarer til nivået i PIPA, se også betraktning 90.

([252]) Se også vedlegg II avsnitt 1.2.

([253]) Se betraktning 158.

([254]) Artikkel 12 i CPPA. Se vedlegg II avsnitt 2.2.2.2.

([255]) Påtalemyndigheten eller polititjenestemannen som gjennomfører de kommunikasjonsbegrensende tiltakene, skal velge den telekommunikasjonen som skal lagres, senest 14 dager etter at tiltakene er avsluttet, og anmode om domstolsgodkjenning (når det gjelder en polititjenestemann, skal anmodningen inngis til en påtalemyndighet, som deretter videresender den til domstolen), se artikkel 12-2 nr. 1 og 2 i CPPA.

([256]) En anmodning om en slik godkjenning skal inneholde informasjon om de kommunikasjonsbegrensende tiltakene, et sammendrag av resultatene av tiltakene, grunnene til lagringen (sammen med dokumentasjon) og telekommunikasjonen som skal lagres (artikkel 12-2 nr. 3 i CPPA). Dersom det ikke inngis en anmodning, skal de innsamlede opplysningene slettes senest 14 dager etter at det kommunikasjonsbegrensende tiltaket er avsluttet (artikkel 12-2 nr. 5 i CPPA), og dersom anmodningen avslås, innen sju dager (artikkel 12-2(5) CPPA). I begge tilfeller skal det innen sju dager inngis en rapport om slettingen til den domstolen som godkjente innsamlingen.

([257]) Artikkel 11 nr. 2 i gjennomføringsdekretet til CPPA.

([258]) Se vedlegg II avsnitt 2.3.

170) For det første er politiet underlagt et internt tilsyn som foretas av en generalinspektør([259]) som foretar lovlighetskontroll, herunder med hensyn til en mulig krenking av menneskerettighetene. Generalinspektøren ble opprettet for å gjennomføre loven om revisjoner i den offentlige sektor, der det oppmuntres til opprettelse av egenrevisjonsorganer og er fastsatt spesifikke krav til hvordan de skal være sammensatt, og hvilke oppgaver de skal ha. I loven er det særlig fastsatt at lederen for et egenrevisjonsorgan skal hentes utenfor den relevante myndigheten (for eksempel tidligere dommere eller professorer) og skal utnevnes for en periode på to til fem år([260]), bare kan avsettes når det er velbegrunnet (for eksempel dersom vedkommende av helsemessige grunner ikke er i stand til å ivareta sine oppgaver, eller er gjenstand for disiplinære tiltak)([261]) og skal garanteres uavhengighet i størst mulig omfang([262]). Ved hindring av en egenrevisjon kan det ilegges administrative bøter([263]). Revisjonsrapporter (som kan omfatte anbefalinger, anmodninger om disiplinære tiltak og anmodninger om erstatning eller korrigering) skal sendes til lederen for den relevante offentlige myndigheten og revisjons- og granskingsutvalget (Board of Audit and Inspection –BAI)([264]) og skal generelt sett offentliggjøres([265]). Resultatene av gjennomføringen av rapporten skal også meddeles BAI([266]) (se betraktning 173 om BAIs tilsynsrolle og myndighet).

171) For det andre fører PIPC tilsyn med at strafferettshåndhevende myndigheters behandling av personopplysninger er i samsvar med PIPA og annen lovgivning som sikrer enkeltpersoners personvern, herunder lover som regulerer innsamlingen av (elektronisk) bevismateriale for strafferettshåndhevende formål, som beskrevet i avsnitt 3.2.1([267]). Ettersom PIPCs tilsyn også omfatter prinsippene om hvorvidt innsamlingen og behandlingen av opplysninger er lovlig og rettferdig (artikkel 3 nr. 1 i PIPA), som ikke overholdes dersom tilgangen til personopplysninger og bruken av disse skjer i strid med disse lovene([268]), kan PIPC også undersøke og sørge for at begrensningene og garantiene beskrevet i avsnitt 3.2.1 overholdes([269]). Ved utøvelsen av denne tilsynsrollen kan PIPC bruke all sin undersøkelsesmyndighet og korrigerende myndighet, som beskrevet nærmere i avsnitt 2.4.2. Allerede før den nylige reformen av PIPA (det vil si i PIPCs tidligere tilsynsrolle for den offentlige sektor) utførte PIPC en rekke tilsynsaktiviteter med henblikk på strafferettshåndhevende myndigheters behandling av personopplysninger, for eksempel i forbindelse med avhør av mistenkte (sak nr. 2013-16 av 26. august 2013), med hensyn til sending av meldinger til enkeltpersoner om ilegging av overtredelsesgebyrer (sak nr. 2015-02-04 av 26. januar 2015), utveksling av opplysninger med andre myndigheter (sak nr. 2018-15-146 av 9. juli 2018, sak nr. 2018-25-308 av 10. desember 2018, sak nr. 2019-02-015 av 29. januar 2019), innsamling av fingeravtrykk eller bilder (sak nr. 2019-17-273 av 9. september 2019), bruken av droner (sak nr. 2020-01-004 av 13. januar 2020). I disse sakene undersøkte PIPC overholdelsen av flere bestemmelser i PIPA (for eksempel lovligheten av behandlingen og prinsippene om formålsbegrensning og dataminimering), men også relevante bestemmelser i andre lover, for eksempel straffeprosessloven, og utstedte ved behov anbefalinger for å bringe behandlingen i samsvar med kravene til vern av opplysninger.

172) For det tredje fører den nasjonale menneskerettighetskommisjonen (National Human Rights Commission – NHRC) uavhengig tilsyn([270]), der den kan undersøke krenkinger av retten til personvern og personvern i forbindelse med korrespondanse som en del av sitt generelle mandat om å verne de grunnleggende rettighetene i artikkel 10–22 i forfatningen. NHRC består av medlemmer som skal inneha spesifikke kvalifikasjoner([271]), og som utnevnes av presidenten i samsvar med lovfestede framgangsmåter. Fire kommisjonsmedlemmer utnevnes etter innstilling fra nasjonalforsamlingen, fire etter innstilling fra presidenten og tre etter innstilling fra høyesterettsjustitiarius([272]). Lederen utnevnes av presidenten blant kommisjonsmedlemmene, og utnevnelsen skal bekreftes av nasjonalforsamlingen([273]). Kommisjonsmedlemmene (herunder lederen) utnevnes for en periode på tre år som kan forlenges, og kan bare avsettes

([259]) Se vedlegg II avsnitt 2.3.1. Se også https://www.police.go.kr/eng/knpa/org/org01.jsp.

([260]) På samme måte utnevnes revisorer på grunnlag av særlige vilkår fastsatt i loven, se artikkel 16 ff. i loven om revisjoner i den offentlige sektor.

([261]) Artikkel 8–11 i loven om revisjoner i den offentlige sektor.

([262]) Artikkel 7 i loven om revisjoner i den offentlige sektor.

([263]) Artikkel 41 i loven om revisjoner i den offentlige sektor.

([264]) Artikkel 23 nr. 1 i loven om revisjoner i den offentlige sektor.

([265]) Artikkel 26 i loven om revisjoner i den offentlige sektor.

([266]) Artikkel 23 nr. 3 i loven om revisjoner i den offentlige sektor.

([267]) Se artikkel 7-8 nr. 3 og 4 og artikkel 7-9 nr. 5 i PIPA.

([268]) Se PIPCs melding 2021-5 avsnitt 6 (vedlegg I).

([269]) Se også vedlegg II avsnitt 2.3.4.

([270]) Artikkel 1 i loven om menneskerettighetskommisjonen (NHRC-loven)

([271]) For å bli utnevnt må et kommisjonsmedlem 1) ha arbeidet i minst ti år ved et universitet eller et godkjent forskningsinstitutt minst som assisterende professor, 2) ha arbeidet som dommer, statsadvokat eller advokat i minst ti år, 3) ha deltatt i menneskerettighetsaktiviteter i minst ti år (for eksempel for en ideell ikke-statlig organisasjon eller internasjonal organisasjon) eller 4) være blitt anbefalt av sivilsamfunnsgrupper (artikkel 5 nr. 3 i NHRC-loven). Etter å ha blitt utnevnt er det dessuten forbudt for kommisjonsmedlemmene å samtidig inneha et verv i nasjonalforsamlingen, i lokale råd eller i en statlig eller lokal myndighet (som offentlig tjenestemann), se artikkel 10 i NHRC-loven.

([272]) Artikkel 5 nr. 1 og 2 i NHRC-loven.

([273]) Artikkel 5 nr. 5 i NHRC-loven.

dersom de idømmes fengselsstraff eller ikke lenger er i stand til å utføre sine oppgaver på grunn av langvarig svekket fysisk eller psykisk funksjonsevne (da skal to tredeler av kommisjonsmedlemmene være enige i avsettelsen)([274]). Som en del av en undersøkelse kan NHRC be om å få framlagt relevant materiale, foreta inspeksjoner og innkalle enkeltpersoner for å avgi vitneforklaring([275]). Når det gjelder myndighet til å treffe utbedringstiltak, kan NHRC utstede (offentlige) anbefalinger for å forbedre eller korrigere spesifikke strategier og spesifikk praksis, som offentlige myndigheter må følge opp med et forslag til gjennomføringsplan([276]). Dersom den aktuelle myndigheten unnlater å gjennomføre anbefalingene, skal den underrette kommisjonen om det([277]), og kommisjonen kan deretter underrette nasjonalforsamlingen om dette og/eller offentliggjøre det. I henhold til den sørkoreanske regjeringens offisielle redegjørelse (vedlegg II avsnitt 2.3.5) følger de sørkoreanske myndighetene generelt sett NHRCs anbefalinger og har et sterkt insentiv til å gjøre det, ettersom gjennomføringen av dem er blitt vurdert å være en del av den generelle løpende evalueringen som gjennomføres under ledelse av statsministerens kontor. Årlige tall som gjelder NHRCs aktiviteter, viser at NHRC fører aktivt tilsyn med strafferettshåndhevende myndigheters aktiviteter, enten på grunnlag av individuelle anmodninger eller undersøkelser på eget initiativ([278]).

173) For det fjerde utføres det generelle tilsynet med lovligheten av offentlige myndigheters aktiviteter av BAI, som gransker statens inntekter og utgifter, men som også mer generelt fører tilsyn med at offentlige myndigheter overholder sine forpliktelser, for å forbedre den offentlige forvaltningen([279]). BAI er formelt opprettet under Republikken Koreas president, men har en uavhengig status med hensyn til oppgavene som skal utføres([280]). Det er dessuten gitt full uavhengighet når det gjelder å utnevne, avsette og organisere sitt personale og utarbeide sitt budsjett([281]). BAI består av en leder (utnevnt av presidenten med nasjonalforsamlingens samtykke)([282]) og seks medlemmer (utnevnt av presidenten på anbefaling fra lederen)([283]) som skal inneha spesifikke lovbestemte kvalifikasjoner([284]), og som bare kan avsettes dersom det reises tiltale eller i tilfelle fengselsstraff eller manglende evne til å ivareta egne oppgaver som følge av langvarig svekket fysisk eller psykisk funksjonsevne([285]). BAI foretar en generell revisjon én gang i året, men kan også foreta spesifikke revisjoner ved spørsmål av særlig interesse. I forbindelse med en revisjon eller inspeksjon kan BAI be om å få framlagt dokumenter og om at visse personer skal være til stede([286]). BAI kan utstede anbefalinger, anmode om disiplinære tiltak eller anmelde forhold([287]).

174) For det femte fører nasjonalforsamlingen parlamentarisk tilsyn med offentlige myndigheter gjennom granskinger og inspeksjoner([288]) av deres aktiviteter([289]). Den kan be om å få utlevert dokumenter, pålegge vitner å møte([290]), anbefale

([274]) Artikkel 7 nr. 1 og artikkel 8 i NHRC-loven.

([275]) Artikkel 36 i NHRC-loven. I henhold til lovens artikkel 6 nr. 7 kan utlevering av materiale eller gjenstander avslås dersom det er fare for at det vil gå ut over statlige konfidensielle forhold som kan ha en vesentlig innvirkning på statens sikkerhet eller diplomatiske forbindelser, eller utgjøre en alvorlig hindring for en strafferettslig etterforskning eller verserende rettssak. I slike tilfeller kan kommisjonen anmode lederen av det relevante organet (som skal etterkomme anmodningen i god tro) om ytterligere informasjon dersom det er nødvendig for å kunne avgjøre om avslaget på å utlevere informasjonen er begrunnet.

([276]) Artikkel 25 nr. 1 og 3 i NHRC-loven.

([277]) Artikkel 25 nr. 4 i NHRC-loven.

([278]) I perioden 2015–2019 mottok NHRC for eksempel mellom 1 380 og 1 699 klager årlig på strafferettshåndhevende myndigheter og behandlet et tilsvarende høyt antall (for eksempel 1 546 klager på politiet i 2018 og 1 249 i 2019). NHRC gjennomførte også flere undersøkelser på eget initiativ som nærmere beskrevet i NHRCs årsrapport for 2018 (tilgjengelig på (https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) og årsrapport for 2019 (tilgjengelig på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([279]) Artikkel 20 og 24 i loven om revisjons- og granskingsutvalget (BAI-loven). Se vedlegg II avsnitt 2.3.2.

([280]) Artikkel 2 nr. 1 i BAI-loven.

([281]) Artikkel 2 nr. 2 i BAI-loven.

([282]) Artikkel 4 nr. 1 i BAI-loven.

([283]) Artikkel 5 nr. 1 og 6 i BAI-loven.

([284]) For eksempel ha arbeidet som dommer, statsadvokat eller advokat i minst ti år, som offentlig tjenestemann eller professor eller i en høyere stilling ved et universitet i minst åtte år eller ha arbeidet i minst ti år i et børsnotert selskap eller en statsfinansiert institusjon (herav minst fem år som administrerende direktør), se artikkel 7 i BAI-loven. Det er dessuten forbudt for medlemmene å delta i politiske aktiviteter og samtidig inneha verv i nasjonalforsamlingen, forvaltningsorganer, organisasjoner som er underlagt BAIs revisjon og inspeksjon, eller andre lønnede verv eller stillinger (artikkel 9 i BAI-loven).

([285]) Artikkel 8 i BAI-loven.

([286]) Se for eksempel artikkel 27 i BAI-loven.

([287]) Artikkel 24 og 31-35 i BAI-loven.

([288]) Artikkel 128 i loven om nasjonalforsamlingen og artikkel 2, 3 og 15 i loven om gransking og undersøkelse av statsforvaltningen. Dette omfatter årlige inspeksjoner av offentlige anliggender generelt, men også gransking av spesifikke saker.

([289]) Se vedlegg avsnitt 2.2.3.

([290]) Artikkel 10 nr. 1 i loven om gransking og undersøkelse av statsforvaltningen. Se også artikkel 128 og 129 loven om nasjonalforsamlingen.

korrigerende tiltak (dersom den fastslår at ulovlige eller urettmessige aktiviteter har funnet sted)([291]) og offentliggjøre resultatene([292]). Dersom nasjonalforsamlingen anmoder om at det treffes korrigerende tiltak, som for eksempel kan omfatte at det gis erstatning, treffes disiplinære tiltak eller at interne prosedyrer forbedres, skal den aktuelle offentlige myndigheten handle uten opphold og rapportere resultatet til nasjonalforsamlingen([293]).

3.2.4 *Prøvings- og klageadgang*

175) I det sørkoreanske systemet er det forskjellige muligheter for å oppnå (rettslig) prøving, herunder mulighet til å oppnå skadeserstatning.

176) For det første gir PIPA enkeltpersoner rett til innsyn i og til retting, sletting og innstilling av behandlingen av personopplysninger som behandles for formål knyttet til strafferettslig håndheving([294]).

177) For det andre kan enkeltpersoner benytte seg av de forskjellige prøvingsmekanismene fastsatt i PIPA dersom deres opplysninger er blitt behandlet av en strafferettshåndhevende myndighet i strid med PIPA eller i strid med begrensningene og garantiene som gjelder for innsamling av personopplysninger i andre lover (det vil si CPA eller CPPA, se betraktning 171). Enkeltpersoner kan klage til PIPC (herunder via personverntelefontjenesten som drives av Republikken Koreas byrå for internett og sikkerhet([295])) eller til utvalget for tvisteløsning i forbindelse med personopplysninger([296]). Disse klagemulighetene omfattes ikke av ytterligere formkrav. På grunnlag av forvaltningsprosessloven kan enkeltpersoner dessuten påklage/bestride PIPCs beslutninger eller unnlatelse av å handle (se betraktning 132).

178) For det tredje kan enhver enkeltperson([297]) klage til NHRC på en sørkoreansk strafferettshåndhevende myndighets krenking av retten til personvern og vern av personopplysninger. NHRC kan anbefale korrigering eller forbedring av relevante lover, institusjoner, retningslinjer eller praksis([298]) eller gjennomføring av tiltak som mekling([299]), opphør av krenkingen av menneskerettighetene, skadeserstatning og tiltak for å hindre at samme eller lignende krenking gjentar seg([300]). I henhold til den sørkoreanske regjeringens offisielle redegjørelse (vedlegg II avsnitt 2.4.2) kan dette også omfatte sletting av ulovlig innsamlede personopplysninger. NHRC har ikke myndighet til å utstede bindende beslutninger, det er i stedet snakk om en mer uformell, rimelig og lett tilgjengelig klageadgang, særlig fordi det som forklart i vedlegg II avsnitt 2.4.2 ikke kreves at det dokumenteres at en skade faktisk har skjedd for at klagen skal bli undersøkt([301]). Dette sikrer at klager fra enkeltpersoner som gjelder innsamling av deres opplysninger, kan undersøkes, selv om enkeltpersonen ikke er i stand til å dokumentere at vedkommendes opplysninger faktisk er blitt samlet inn (for eksempel fordi de ennå ikke er blitt underrettet). Det framgår av NHRCs årlige aktivitetsrapporter at enkeltpersoner også benytter seg av denne muligheten i praksis for å stille spørsmål ved strafferettshåndhevende myndigheters aktiviteter, herunder deres behandling av personopplysninger([302]). Dersom en person ikke er tilfreds med utfallet av

([291]) Artikkel 16 nr. 2 i loven om gransking og undersøkelse av statsforvaltningen.

([292]) Artikkel 12-2 i loven om gransking og undersøkelse av statsforvaltningen.

([293]) Artikkel 16 nr. 3 i loven om gransking og undersøkelse av statsforvaltningen.

([294]) Denne retten kan utøves direkte overfor vedkommende myndighet eller indirekte via PIPC (artikkel 35 nr. 2 i PIPA). Som nærmere beskrevet i betraktning 76–78 får unntak fra disse rettighetene bare anvendelse når det er nødvendig for å beskytte viktige (offentlige) interesser.

([295]) Artikkel 62 i PIPA.

([296]) Artikkel 40–50 i PIPA og artikkel 48-2 til 57 i gjennomføringsdekretet til PIPA. Se også vedlegg II avsnitt 2.4.1.

([297]) Som forklart i vedlegg II avsnitt 2.4.2 skal begrepet «bosatt» ses i sammenheng med begrepet «jurisdiksjon» og ikke «territorium», selv om det i artikkel 4 i NHRC-loven vises til statsborgere og utlendinger bosatt i Republikken Korea. Dersom de grunnleggende rettighetene til en utlending bosatt utenfor Republikken Korea krenkes av nasjonale institusjoner i Republikken Korea, kan den aktuelle personen derfor klage til NHRC. Dette vil være tilfellet dersom sørkoreanske offentlige myndigheter har ulovlig tilgang til en utlendings personopplysninger som er overført til Republikken Korea. Se særlig forklaringene på https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.

([298]) Artikkel 44 i NHRC-loven.

([299]) En person kan også be om å få løst klagesaken gjennom mekling, se artikkel 42 ff. i NHRC-loven.

([300]) Artikkel 42 nr. 4 i NHRC-loven. NHRC kan dessuten vedta hastetiltak ved en pågående overtredelse som det er sannsynlig vil forårsake skade som er vanskelig å avhjelpe dersom det ikke gripes inn, se artikkel 48 i NHRC-loven.

([301]) En klage skal i prinsippet inngis innen et år etter overtredelsen, men NHRC kan beslutte å undersøke en klage som inngis etter denne fristen, så lenge foreldelsesfristen i henhold til straffe- eller sivilretten ikke er utløpt (artikkel 32 nr. 1 pkt. 4 i NHRC-loven).

([302]) NHRC har for eksempel tidligere behandlet klager og utstedt anbefalinger angående ulovlig beslaglegging og manglende oppfyllelse av kravet om å underrette berørte personer om en beslaglegging (se s. 80 og 91 i NHRCs årsrapport for 2018 på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), samt politiets, påtalemyndighetens og domstolenes ulovlige behandling av personopplysninger (se s. 157–158 i NHRCs årsrapport for 2019 på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308 og s. 76 i årsrapporten for 2019 på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

prosedyren ved NHRC, kan vedkommende klage inn NHRCs beslutninger (for eksempel en beslutning om ikke å fortsette undersøkelsen av en klage([303])) og anbefalinger til de sørkoreanske domstolene i henhold til forvaltningsprosessloven (se betraktning 181)([304]). En prosedyre ved NHRC kan dessuten lette adgangen til domstolene ytterligere, ettersom en person kan anlegge sak mot den offentlige myndigheten som har behandlet vedkommendes opplysninger ulovlig, på grunnlag av NHRC konklusjoner og i samsvar med prosedyrene beskrevet i betraktning 181–183.

179) For det fjerde finnes det forskjellige rettsmidler som gir enkeltpersoner mulighet til å påberope seg begrensningene og garantiene beskrevet i avsnitt 3.2.1 for å oppnå prøving([305]).

180) Når det gjelder beslaglegging (herunder av opplysninger), gir CPA mulighet til å protestere mot eller bestride iverksettingen av en kjennelse gjennom en «kvasiklage» ved å anmode vedkommende domstol om å annullere eller endre en disposisjon som en representant for påtalemyndigheten eller polititjenestemann har truffet([306]).

181) Mer generelt kan enkeltpersoner bestride offentlige myndigheters tiltak([307]) eller unnlatelse av å handle([308]) (herunder strafferettshåndhevende myndigheter) i henhold til forvaltningsprosessloven([309]). Et administrativt tiltak anses som en «disposisjon som kan bestrides» dersom den har direkte innvirkning på borgerrettigheter og -plikter([310]), noe som, som bekreftet av den sørkoreanske regjeringen (vedlegg II avsnitt 2.4.3), er tilfellet for tiltak for å samle inn personopplysninger, enten direkte (for eksempel ved avlytting av kommunikasjon), gjennom bindende anmodninger om utlevering (for eksempel til en tjenesteleverandør) eller anmodninger om frivillig samarbeid. For at en klage i henhold til forvaltningsprosessloven skal kunne behandles, må en enkeltperson ha en rettslig interesse av å forfølge klagen([311]). I henhold til høyesteretts rettspraksis fortolkes «rettslig interesse» som «en rettslig beskyttet interesse», det vil si en direkte og spesifikk interesse som er beskyttet av lover og forskrifter, og som administrative bestemmelser er basert på (det vil si ikke allmennhetens generelle, indirekte og abstrakte interesser)([312]). Enkeltpersoner har en slik rettslig interesse ved overtredelse av begrensningene og garantiene som gjelder for innsamling av deres personopplysninger for formål knyttet til strafferettslig håndheving (i henhold til spesifikke lover eller PIPA). På grunnlag av forvaltningsprosessloven kan en domstol beslutte å tilbakekalle eller endre en ulovlig disposisjon, utstede en avgjørelse om ugyldighet (det vil si om at disposisjonen ikke har rettsvirkning eller ikke eksisterer i rettsordenen) eller om at en unnlatelse av å handle er ulovlig([313]). En endelig dom avsagt i henhold til forvaltningsprosessloven er bindene for partene([314]).

([303]) Dersom NHRC for eksempel unntaksvis ikke kan inspisere visse materialer eller fasiliteter fordi de gjelder statshemmeligheter som kan ha en vesentlig innvirkning på statens sikkerhet eller diplomatiske forbindelser, eller dersom inspeksjonen vil utgjøre en alvorlig hindring for en strafferettslig etterforskning eller verserende rettssak, og dersom dette hindrer NHRC i å foreta undersøkelsen som kreves for å vurdere om den mottatte klagen er begrunnet, vil NHRC underrette den berørte personen om grunnene til at klagen ble avvist, i samsvar med artikkel 39 i NHRC-loven. I dette tilfellet kan enkeltpersonen bestride NHRCs beslutning i henhold til forvaltningsprosessloven.

([304]) Se for eksempel Seouls høyere domstols avgjørelse 2007Nu27259 av 18. april 2008 bekreftet av høyesteretts avgjørelse 2008Du7854 av 9. oktober 2008, Seouls høyesteretts avgjørelse 2017Nu69382 av 2. februar 2018.

([305]) Se vedlegg II avsnitt 2.4.3.

([306]) Artikkel 417 sammenholdt med artikkel 414 nr. 2 i CPA. Se også høyesteretts avgjørelse 97Mo66 av 29. september 1997.

([307]) I forvaltningsprosessloven vises det til en «disposisjon», det vil si utøvelse eller avvisning av å utøve offentlig myndighet i en bestemt sak.

([308]) I henhold til forvaltningsprosessloven gjelder dette et forvaltningsorgans langvarige unnlatelse av å treffe en bestemt disposisjon i strid med en rettslig forpliktelse til å gjøre det.

([309]) En administrativ prøving kan i første omgang bringes inn for administrative klageutvalg nedsatt under visse offentlige myndigheter (for eksempel NIS og NHRC) eller for det sentrale administrative klageutvalget nedsatt under kommisjonen for korrupsjonsbekjempelse og borgerrettigheter (artikkel 6 i loven om administrative klager og artikkel 18 nr. 1 i forvaltningsprosessloven) som en mer uformell mulighet til prøving. Et krav kan også bringes direkte inn for de sørkoreanske domstolene på grunnlag av forvaltningsprosessloven.

([310]) Høyesteretts avgjørelse 98Du18435 av 22. oktober 1999, høyesteretts avgjørelse 99Du1113 av 8. september 2000 og høyesteretts avgjørelse 2010Du3541 av 27. september 2012.

([311]) Artikkel 12, 35 og 36 i forvaltningsprosessloven. Dessuten skal en anmodning om tilbakekalling/endring av en disposisjon og en anmodning om å få bekreftet at en unnlatelse av å handle er ulovlig, inngis senest 90 dager etter den datoen personen får kjennskap til disposisjonen/unnlatelsen, og i prinsippet senest et år etter datoen for utstedelse av disposisjonen eller unnlatelsen, med mindre det foreligger berettigede grunner (artikkel 20 og 38 nr. 2 i forvaltningsprosessloven). Begrepet «berettigede grunner» er blitt fortolket i vid forstand av høyesterett og krever en vurdering av om det er samfunnsmessig akseptabelt å tillate å bringe inn en forsinket klage i lys av alle sakens omstendigheter (høyesteretts avgjørelse 90Nu6521 av 28. juni 1991). Som bekreftet av den sørkoreanske regjeringen i vedlegg II avsnitt 2.4.3 omfatter dette (men er ikke begrenset til) grunner til forsinkelsen som den berørte parten ikke kan holdes ansvarlig for (det vil si situasjoner som ligger utenfor klagerens kontroll, for eksempel dersom vedkommende ikke er blitt underrettet om innsamlingen av vedkommendes personopplysninger) eller force majeure (for eksempel en naturkatastrofe eller krig).

([312]) Høyesteretts avgjørelse 2006Du330 av 26. mars 2006.

([313]) Artikkel 2 og 4 i forvaltningsprosessloven.

([314]) Artikkel 30 nr. 1 i forvaltningsprosessloven.

182) I tillegg til å bestride statlig tiltak ved å anlegge en forvaltningssak kan enkeltpersoner også inngi en forfatningsmessig klage til forfatningsdomstolen angående en eventuell krenking av deres grunnleggende rettigheter som følge av utøvelse eller manglende utøvelse av offentlig myndighet (unntatt domstolsavgjørelser)([315]). Dersom andre rettsmidler er tilgjengelige, skal disse være uttømt først. I henhold til forfatningsdomstolens rettspraksis kan fremmede borgere inngi en forfatningsmessig klage i den grad deres grunnleggende rettigheter er anerkjent i den sørkoreanske forfatningen (se forklaringene i avsnitt 1.1)([316]). Forfatningsdomstolen kan ugyldiggjøre utøvelsen av offentlig myndighet som forårsaket overtredelsen, eller bekrefte at en bestemt unnlatelse av å handle er forfatningsstridig([317]). Da skal den relevante myndigheten treffe tiltak for å etterkomme domstolens avgjørelse.

183) Enkeltpersoner kan dessuten oppnå skadeserstatning ved de sørkoreanske domstolene. Dette omfatter først og fremst muligheten til å kreve erstatning for overtredelser av PIPA som er begått av strafferettshåndhevende myndigheter, i samsvar med artikkel 39 (se også betraktning 135). Mer generelt kan enkeltpersoner søke om erstatning for skader som offentlig tjenestemenn har forårsaket under utøvelse av offisielle oppgaver i strid med loven, på grunnlag av loven om statlig erstatning (se også betraktning 135)([318]).

184) Mekanismene beskrevet i betraktning 176–183 gir de registrerte mulighet til effektiv administrativ og rettslige prøving, som særlig setter dem i stand til å gjøre sine rettigheter gjeldende, herunder retten til innsyn i egne personopplysninger eller til å få rettet eller slettet slike opplysninger.

3.3 **Sørkoreanske offentlige myndigheters tilgang til og bruk av personopplysninger for formål knyttet til nasjonal sikkerhet**

185) Republikken Koreas lovgivning inneholder en rekke begrensninger og garantier med hensyn til tilgangen til og bruken av personopplysninger for formål knyttet til nasjonal sikkerhet samt en rekke tilsyns- og prøvingsmekanismer som oppfyller kravene nevnt i betraktning 141–143 i denne beslutningen. Vilkårene for slik tilgang og garantiene som gjelder for utøvelse av denne myndigheten, beskrives nærmere i avsnittene nedenfor.

3.3.1 *Rettslig grunnlag, begrensninger og garantier*

186) I Republikken Korea kan det gis tilgang til personopplysninger for formål knyttet til nasjonal sikkerhet på grunnlag av CPPA, TBA og loven om terrorbekjempelse og beskyttelse av borgere og den offentlige sikkerhet (antiterrorloven)([319]). Hovedmyndigheten([320]) med kompetanse på området nasjonal sikkerhet er den nasjonale etterretningstjenesten (National Intelligence Service – NIS)([321]). NIS skal i forbindelse med innsamling og bruk av personopplysninger oppfylle

([315]) Artikkel 68 nr. 1 i loven om forfatningsdomstolen. Forfatningsmessige klager skal inngis senest 90 dager etter at personen har fått kjennskap til overtredelsen, og senest et år etter at den har funnet sted. Som det også forklares i vedlegg II avsnitt 2.4.3. vil en klage fremdeles kunne tas opp til behandling dersom det foreligger «berettigede grunner» som fortolket i samsvar med høyesteretts rettspraksis beskrevet i fotnote 312, ettersom prosedyren i forvaltningsprosessloven får anvendelse på tvister i henhold til artikkel 40 i loven om forfatningsdomstolen. Dersom andre rettsmidler må uttømmes først, skal en forfatningsmessig klage inngis senest 30 dager etter den endelige avgjørelsen om et slikt rettsmiddel (artikkel 69 i loven om forfatningsdomstolen).

([316]) Forfatningsdomstolens avgjørelse 99HeonMa194 av 29. november 2001.

([317]) Artikkel 75 nr. 3 i loven om forfatningsdomstolen.

([318]) Artikkel 2 nr. 1 i loven om statlig erstatning.

([319]) Se vedlegg II avsnitt 3.1.

([320]) Politiet og påtalemyndigheter kan også unntaksvis samle inn personopplysninger for formål knyttet til nasjonal sikkerhet (se fotnote 327 og vedlegg II avsnitt 3.2.1.2). I tillegg har Republikken Koreas militære etterretningsorgan (forsvarssikkerhetskommandoen opprettet under forsvarsdepartementet) myndighet på området nasjonal sikkerhet. Som forklart i vedlegg II avsnitt 3.1 har den imidlertid bare ansvar for militær etterretning og overvåker bare sivile når det er nødvendig for å ivareta de militære funksjonene den har. Den kan bare etterforske militært personell, sivilt ansatte i militæret, personer under militær opplæring, reservister, rekrutter og krigsfanger (artikkel 1 i loven om militærdomstolen). Når forsvarssikkerhetskommandoen samler inn kommunikasjonsopplysninger for formål knyttet til nasjonal sikkerhet, er den underlagt begrensningene og garantiene fastsatt i CPPA og gjennomføringsdekretet til den.

([321]) NIS' mandat er å samle inn, kompilere og spre informasjon om andre land (det vil si generell informasjon om tendenser og utvikling i andre land eller statlige aktørers aktiviteter), etterretning knyttet til kontraspionasje (herunder militær- og industrispionasje), terrorisme og internasjonale kriminelle syndikaters aktiviteter, etterretning om visse typer straffbare handlinger rettet mot offentlig og nasjonal sikkerhet (for eksempel innenlandsk opprør, aggresjon utenfra) og etterretning knyttet til oppgavene med å sikre cybersikkerheten og forebygge eller bekjempe cyberangrep og -trusler (artikkel 4 nr. 2 i NIS-loven). Se også vedlegg II avsnitt 3.1.

relevante rettslige krav (herunder PIPA og CPPA)([322]) og generelle retningslinjer utarbeidet av presidenten og gjennomgått av nasjonalforsamlingen([323]). NIS skal som et generelt prinsipp være politisk nøytralt og beskytte enkeltpersoners rettigheter og friheter([324]). Ansatte i NIS må dessuten ikke misbruke sin offisielle myndighet til å tvinge en institusjon, organisasjon eller enkeltperson til å gjøre noe de ikke er forpliktet til (ved lov), eller hindre en person i å utøve sine rettigheter([325]).

3.3.1.1 Tilgang til kommunikasjonsopplysninger

187) Sørkoreanske offentlige myndigheter([326]) kan på grunnlag av CPPA samle inn kommunikasjonsbekreftelsesdata (det vil si datoen og start- og sluttidspunktet for telekommunikasjoner, antall utgående og innkommende samtaler samt den andre partens abonnentnummer, bruksfrekvens, loggfiler om bruken av telekommunikasjonstjenester og lokaliseringsopplysninger, se betraktning 155) og kommunikasjonsinnhold (ved hjelp av kommunikasjonsbegrensende tiltak, se betraktning 155) for formål knyttet til nasjonal sikkerhet (som fastsatt i NIS' mandat, se fotnote 322). Denne myndigheten omfatter to typer opplysninger: 1) Kommunikasjon der den ene eller begge parter er sørkoreanske statsborgere([327]), og 2) kommunikasjon fra a) land som er fiendtlig innstilte mot Republikken Korea, b) utenlandske organer, grupper eller statsborgere som mistenkes for å delta i aktiviteter som kan skade Republikken Korea([328]), eller c) medlemmer av grupper som opererer på Koreahalvøya, men uten reelt å være underlagt Republikken Koreas suverenitet, og deres paraplygrupper basert i andre land([329]). EU-borgeres kommunikasjon som overføres fra Unionen til Republikken Korea på grunnlag av denne beslutningen, kan derfor bare samles inn i henhold til CPPA for formål knyttet til nasjonal sikkerhet (med forbehold for vilkårene fastsatt i betraktning 188–192) dersom den enten er mellom en EU-borger og en sørkoreansk statsborger, eller, dersom den utelukkende er mellom ikke-sørkoreanske statsborgere, dersom den faller inn under en av de tre ovennevnte kategoriene 2 a), b) og c).

188) I begge scenarioer kan innsamling av kommunikasjonsbekreftelsesdata bare skje for å forebygge trusler mot den nasjonale sikkerheten([330]), og det kan bare treffes kommunikasjonsbegrensende tiltak dersom det foreligger en alvorlig risiko for den nasjonale sikkerheten og innsamlingen er nødvendig for å avverge den([331]). Det kan i tillegg bare gis tilgang til kommunikasjonsinnhold som en siste utvei, og det skal gjøres en innsats for å minimere krenkingen av personvernet i forbindelse med kommunikasjon([332]) og på den måten sikre at dette står i et rimelig forhold til formålet knyttet til nasjonal sikkerhet som forfølges. Innsamlingen av både kommunikasjonsinnhold og kommunikasjonsbekreftelsesdata kan pågå i høyst fire måneder og må umiddelbart opphøre dersom målet som forfølges, nås tidligere([333]). Dersom de relevante vilkårene fortsatt er oppfylt, kan perioden forlenges med opptil fire måneder med forhåndstillatelse fra en domstol (for tiltakene beskrevet i betraktning 189) eller presidenten (for tiltakene beskrevet i betraktning 190)([334]).

189) De samme prosessuelle garantiene gjelder for innsamling av kommunikasjonsbekreftelsesdata og kommunikasjonsinnhold([335]). Dersom minst en av personene som er involvert i kommunikasjonen, er sørkoreansk statsborger, skal etterretningsorganet inngi en skriftlig anmodning til den høyere påtalemyndigheten, som deretter skal framsette en

([322]) Se også artikkel 14, 22 og 23 i NIS-loven.
([323]) Artikkel 4 nr. 2 i NIS-loven.
([324]) Artikkel 3 nr. 1, artikkel 6 nr. 2 og artikkel 11 og 21 i NIS-loven. Se også reglene for interessekonflikter, særlig artikkel 10 og 12 i NIS-loven.
([325]) Artikkel 13 i NIS-loven.
([326]) Dette omfatter etterretningsorganene (det vil si NIS og forsvarssikkerhetskommandoen) og politi/påtalemyndighet.
([327]) Artikkel 7 nr. 1 pkt. 1 i CPPA.
([328]) I henhold til den sørkoreanske regjeringens forklaring i fotnote 244 i vedlegg II dreier det seg om aktiviteter som truer nasjonens eksistens og sikkerhet, den demokratiske orden eller folkets overlevelse og frihet.
([329]) Artikkel 7 nr. 1 pkt. 2 i CPPA.
([330]) Artikkel 13-4 i CPPA.
([331]) Artikkel 7 nr. 1 i CPPA.
([332]) Artikkel 3 nr. 2 i CPPA. Kommunikasjonsbegrensende tiltak skal dessuten umiddelbart opphøre når de ikke lenger er nødvendige, slik at enhver krenking av den enkeltes rett til kommunikasjonshemmelighet begrenses til et minimum (artikkel 2 i gjennomføringsdekretet til CPPA).
([333]) Artikkel 7 nr. 2 i CPPA.
([334]) Søknaden om å få godkjent en forlengelse av overvåkingstiltakene skal inngis skriftlig med en angivelse av grunnene til at det bes om forlengelse, og det skal vedlegges dokumentasjon (artikkel 7 nr. 2 i CPPA og artikkel 5 i gjennomføringsdekretet til CPPA).
([335]) Se artikkel 13-4 nr. 2 i CPPA og artikkel 37 nr. 4 i gjennomføringsdekretet til CPPA, der det er fastsatt at prosedyrene som gjelder for innsamling av kommunikasjonsinnhold, også gjelder for innsamling av kommunikasjonsbekreftelsesdata. Se også vedlegg II avsnitt 3.2.1.1.1.

begjæring om kjennelse for en overdommer ved en høyere domstol([336]). I CPPA er det angitt hvilke opplysninger som skal angis i begjæringen til påtalemyndigheten, begjæringen om kjennelse og selve kjennelsen, herunder særlig begrunnelsen for begjæringen og de viktigste grunnene til mistanke, dokumentasjon og informasjon om formålet, målet (det vil si den eller de berørte personene), omfanget og varigheten av det foreslåtte tiltaket([337]). Innsamling uten kjennelse må bare skje dersom det dreier seg om en sammensvergelse som truer den nasjonale sikkerheten, og det foreligger en nødssituasjon som gjør det umulig å gjennomføre de ovennevnte prosedyrene([338]). Også i dette tilfellet skal det imidlertid framsettes en begjæring om kjennelse umiddelbart etter at tiltaket er truffet([339]). CPPA definerer derfor tydelig omfanget av og vilkårene for disse typene innsamling, og de er underlagt spesifikke (prosessuelle) garantier (herunder rettslig forhåndsgodkjenning) som sikrer at bruken av slike tiltak begrenses til det som er nødvendig og forholdsmessig. Kravet om at det skal gi detaljert informasjon i både begjæringen om kjennelse og selve kjennelsen, utelukker dessuten muligheten for vilkårlig tilgang.

190) Når det gjelder kommunikasjon mellom ikke-sørkoreanske statsborgere som omfattes av en av de tre spesifikke kategoriene angitt i betraktning 187, skal det inngis en søknad til direktøren for NIS, som etter å ha vurdert hvor egnet de foreslåtte tiltakene er, skal be om en skriftlig forhåndsgodkjenning fra Republikken Koreas president([340]). Søknaden som utarbeides av etterretningsorganet, skal inneholde den samme detaljerte informasjonen som en begjæring om rettskjennelse (se betraktning 189), særlig om begrunnelsen for begjæringen og de viktigste grunnene til mistanke, dokumentasjon og informasjon om målene for og omfanget og varigheten av de foreslåtte tiltakene samt den eller de berørte personene som de er rettet mot([341]). I nødssituasjoner([342]) skal det innhentes forhåndsgodkjenning fra ministeren som det relevante etterretningsorganet er underlagt, selv om etterretningsorganet må søke om godkjenning fra presidenten umiddelbart etter at hastetiltakene er truffet([343]). Også når det gjelder innsamling av kommunikasjon mellom utelukkende ikke-sørkoreanske statsborgere, begrenser CPPA derfor bruken av slike tiltak til det som er nødvendig og forholdsmessig ved tydelig å avgrense de begrensede kategoriene av personer som kan omfattes av slike tiltak, og ved å fastsette detaljerte kriterier som etterretningsorganer må vise at de oppfyller, for å begrunne søknaden om innsamling av opplysninger. Dette utelukker også muligheten for vilkårlig tilgang. Selv om det ikke foreligger en uavhengig forhåndsgodkjenning av slike tiltak, fører PIPC og NHRC uavhengig etterhåndstilsyn (se for eksempel betraktning 199–200).

191) I CPPA er det dessuten fastsatt en rekke andre garantier som bidrar til etterhåndstilsyn, og som forenkler enkeltpersoners tilgang til effektive rettsmidler. For det første er det i CPPA fastsatt forskjellige registrerings- og rapporteringskrav i forbindelse med enhver form for innsamling for formål knyttet til den nasjonale sikkerheten. Etterretningsorganer som ber private operatører om å samarbeide, skal særlig innhente en rettskjennelse / tillatelse fra presidenten eller en kopi av forsiden på en erklæring om sensur i nødssituasjoner som den aktuelle enheten skal ta vare på([344]). Dersom private aktører tvinges til å samarbeide, skal både den anmodende offentlige myndigheten og den

([336]) Artikkel 6 nr. 5 og 8, artikkel 7 nr. 1 pkt. 1 og artikkel 7 nr. 3 i CPPA sammenholdt med artikkel 7 nr. 3–4 i gjennomføringsdekretet til CPPA.

([337]) Se artikkel 7 nr. 3 og artikkel 6 nr. 4 i CPPA (for etterretningsorganets begjæring), artikkel 4 i gjennomføringsdekretet til CPPA (for påtalemyndighetens begjæring) og artikkel 7 nr. 3 og artikkel 6 nr. 6 i CPPA (for kjennelsen).

([338]) Artikkel 8 i CPPA.

([339]) Artikkel 8 nr. 2 og 8 i CPPA. Innsamlingen skal opphøre umiddelbart dersom rettskjennelsen ikke oppnås senest 36 timer etter at tiltakene er truffet. Dersom overvåkingen avsluttes i løpet av kort tid og uten en rettskjennelse, skal lederen for vedkommende høyere påtalemyndighet sende en melding om hastetiltak utarbeidet av etterretningsorganet til lederen for vedkommende domstol, som på dette grunnlaget kan undersøke om innsamlingen er lovlig (artikkel 8 nr. 5 og 7 i CPPA). I denne meldingen angis formålet, målet, omfanget, varigheten, gjennomføringsstedet og overvåkingsmetoden samt grunnene til at det ikke ble inngitt en begjæring før tiltakene ble truffet (artikkel 8 nr. 6 i CPPA). Mer generelt kan etterretningsorganene bare treffe hastetiltak i samsvar med en «erklæring om sensur/avlytting i nødssituasjoner», og de skal føre registre over slike tiltak (artikkel 8 nr. 4 i CPPA).

([340]) Artikkel 8 nr. 1 og 2 i gjennomføringsdekretet til CPPA.

([341]) Artikkel 8 nr. 3 i gjennomføringsdekretet til CPPA, sammenholdt med artikkel 6 nr. 4 i CPPA.

([342]) Det vil si når tiltakene gjelder en sammensvergelse som truer den nasjonale sikkerheten, og det ikke er tilstrekkelig tid til å innhente godkjenning fra presidenten og manglende hastetiltak kan skade den nasjonale sikkerheten (artikkel 8 nr. 8 i CPPA).

([343]) Artikkel 8 nr. 9 i CPPA. Innsamlingen skal opphøre umiddelbart dersom tillatelsen ikke oppnås senest 36 timer etter at søknaden ble inngitt.

([344]) Artikkel 9 nr. 2 i CPPA og artikkel 12 i gjennomføringsdekretet til CPPA. Se artikkel 13 i gjennomføringsdekretet til CPPA om muligheten til å kreve bistand fra postkontorer og leverandører av telekommunikasjonstjenester. Private operatører som anmodes om å utlevere opplysninger, kan nekte å gjøre det dersom kjennelsen/godkjenningen eller erklæringen om sensur i nødssituasjoner inneholder en feil identifikator (for eksempel et telefonnummer som tilhører en annen person enn den identifiserte personen). Under alle omstendigheter er det forbudt å utlevere passord som brukes til kommunikasjon (artikkel 9 nr. 4 i CPPA).

relevante operatøren føre registre over formålet med og gjenstanden for tiltakene samt datoen for gjennomføringen([345]). I tillegg skal etterretningsorganene rapportere om opplysningene de har samlet inn, og om utfallet av overvåkingen, til direktøren for NIS([346]).

192) For det andre skal enkeltpersoner underrettes om innsamlingen av deres opplysninger (kommunikasjonsbekreftelsesdata eller kommunikasjonsinnhold) for formål knyttet til nasjonal sikkerhet dersom innsamlingen gjelder kommunikasjon der minst en av partene er sørkoreansk statsborger([347]). Underretningen skal skje skriftlig senest 30 dager etter at innsamlingen ble avsluttet (herunder dersom opplysningene ble samlet inn i henhold til hasteprosedyrer), og den kan bare utsettes dersom og så lenge det bringer den nasjonale sikkerheten i fare eller kan skade menneskers liv og fysiske sikkerhet([348]). Uavhengig av denne underretningen har enkeltpersoner tilgang til forskjellige prøvings- og klagemuligheter, som nærmere forklart i avsnitt 3.3.4.

3.3.1.2 Innsamling av opplysninger om terrormistenkte

193) I henhold til antiterrorloven kan NIS samle inn opplysninger om terrormistenkte([349]) i samsvar med begrensningene og garantiene fastsatt i andre lover([350]). NIS kan særlig innhente kommunikasjonsopplysninger (på grunnlag av CPPA) og andre personopplysninger (gjennom en anmodning om frivillig utlevering)([351]). Når det gjelder innsamling av kommunikasjonsopplysninger (det vil si kommunikasjonsinnhold eller kommunikasjonsbekreftelsesdata), får begrensningene og garantiene beskrevet i avsnitt 3.3.1.1 anvendelse, herunder kravet om at det skal innhentes en rettskjennelse. Når det gjelder anmodninger om frivillig utlevering av andre typer personopplysninger om terrormistenkte, må NIS oppfylle kravene i forfatningen og PIPA som gjelder nødvendighet og forholdsmessighet (se betraktning 164)([352]). Behandlingsansvarlige som mottar slike anmodninger, kan etterkomme dem frivillig i henhold til vilkårene fastsatt i PIPA (for eksempel i samsvar med prinsippet om dataminimering og ved å begrense innvirkningen på den enkeltes personvern)([353]). I så fall skal de også oppfylle kravet om at den berørte personen skal underrettes, som følger av melding 2021-5 (se betraktning 166).

([345]) Når det gjelder kommunikasjonsbegrensende tiltak, skal slike registre oppbevares i tre år, se artikkel 9 nr. 3 i CPPA og artikkel 17 nr. 2 i gjennomføringsdekretet til CPPA. Når det gjelder kommunikasjonsbekreftelsesdata, skal etterretningsorganene føre registre over at det er inngitt en anmodning om slike data, og over selve den skriftlige anmodningen og institusjonen som baserte seg på den (artikkel 13 nr. 5 og artikkel 13-4 nr. 3 i CPPA). Leverandører av telekommunikasjonstjenester skal oppbevare registrene i sju år og rapportere to ganger i året til ministeren for vitenskap og IKT om frekvensen av slike utleveringer (artikkel 9 nr. 3 i CPPA sammenholdt med artikkel 13 nr. 7 i CPPA og artikkel 37 nr. 4 og artikkel 39 i gjennomføringsdekretet til CPPA).

([346]) Artikkel 18 nr. 3 i gjennomføringsdekretet til CPPA.

([347]) Artikkel 9-2 nr. 3 og artikkel 13-4 i CPPA. I underretningen skal følgende angis: 1) At opplysninger er samlet inn, 2) hvem som har samlet dem inn, og 3) gjennomføringsperioden.

([348]) Artikkel 9-2 nr. 4 i CPPA. I så fall skal underretningen skje senest 30 dager etter at grunnene til utsettelsen ikke lenger foreligger, se artikkel 13-4 nr. 2 og artikkel 9-2 nr. 6 i CPPA.

([349]) Det vil si medlemmer av en terrorgruppe (som definert av De forente nasjoner, se artikkel 2 nr. 2 i antiterrorloven), personer som fremmer og sprer en terrorgruppes ideer eller taktikk, samler inn penger til eller bidrar til finansiering av terrorisme eller deltar i andre aktiviteter som planlegging av, sammensvergelse til, spredning av propaganda om eller oppmuntring til terrorisme, eller personer der det foreligger begrunnet mistanke om at de allerede har utført slike aktiviteter (artikkel 2 nr. 3 i antiterrorloven). «Terrorisme» defineres i artikkel 2 nr. 1 i antiterrorloven som handlinger som utføres med det formål å hindre statens, en lokal myndighets eller en utenlandsk regjerings myndighetsutøvelse (herunder internasjonale organisasjoner), å tvinge dem til å treffe tiltak uten at de er rettslig forpliktet til det, eller true allmennheten. Slike handlinger kan for eksempel omfatte drap, kidnapping eller gisseltaking, kapring / ulovlig beslaglegging eller ødeleggelse av eller skade på et skip eller et luftfartøy, bruk av biokjemiske eller eksplosive våpen eller brannvåpen med det formål å forårsake død, alvorlig personskade eller skade på eiendom og misbruk av kjernefysisk eller radioaktivt materiale.

([350]) Artikkel 9 nr. 1 og 3 i antiterrorloven.

([351]) I antiterrorloven vises det også til muligheten for å samle inn opplysninger om innreise til og utreise fra Republikken Korea på grunnlag av immigrasjonsloven og tolloven, men det er i dag ikke fastsatt en slik myndighet i disse lovene (se vedlegg II avsnitt 3.2.2.1). De vil uansett i prinsippet ikke få anvendelse på opplysninger som overføres på grunnlag av denne beslutningen, ettersom de normalt gjelder opplysninger som samles inn direkte av sørkoreanske myndigheter (og ikke tilgang til opplysninger som tidligere er overført fra Unionen til sørkoreanske behandlingsansvarlige). I antiterrorloven angis dessuten ARUSFTI som rettslig grunnlag for innsamling av opplysninger om finansielle transaksjoner. Som forklart i fotnote 200 omfattes de typene opplysninger som kan innhentes på grunnlag av denne loven, imidlertid ikke av denne beslutningens virkeområde. I antiterrorloven er det også fastsatt at NIS kan samle inn lokaliseringsopplysninger gjennom ikke-bindende anmodninger, og at leverandører av lokaliseringsopplysninger da frivillig kan utlevere slike opplysninger på vilkårene fastsatt i PIPA (som beskrevet i betraktning 193) og i lokaliseringsopplysningsloven. Som forklart i fotnote 17 vil lokaliseringsopplysninger imidlertid ikke bli overført fra Unionen til sørkoreanske behandlingsansvarlige på grunnlag av denne beslutningen, men vil bli generert i Republikken Korea.

([352]) Se vedlegg II avsnitt 3.2.2.2.

([353]) Se artikkel 58 nr. 4 i PIPA der det er fastsatt at personopplysninger skal behandles i så lite omfang som nødvendig for å oppfylle det tiltenkte formålet, og artikkel 3 nr. 6 i PIPA der det er fastsatt at personopplysninger skal behandles på en måte som minimerer risikoen for å krenke den enkeltes rett til personvern. Se også artikkel 59 pkt. 2 og 3 i PIPA der det er fastsatt at det for behandlingsansvarlige er forbudt å utlevere personopplysninger til tredjeparter uten tillatelse.

3.3.1.3 Anmodninger om frivillig utlevering av abonnentopplysninger

194) Telekommunikasjonsleverandører kan på grunnlag av TBA frivillig utlevere abonnentopplysninger (se betraktning 163) på anmodning fra et etterretningsorgan som har til hensikt å samle inn slike opplysninger for å avverge en trussel mot den nasjonale sikkerheten([354]). For slike anmodninger fra NIS gjelder de samme begrensningene (som følger av forfatningen, PIPA og TBA) som på området strafferettslig håndheving, som fastsatt i betraktning 164([355]). Telekommunikasjonsleverandører plikter ikke å etterkomme slike anmodninger og kan bare gjøre dette i henhold til vilkårene fastsatt i PIPA (særlig i samsvar med prinsippet om dataminimering og ved å begrense innvirkningen på den enkeltes rett til personvern, se også betraktning 193). Det gjelder samme krav til registrering og underretning av den berørte personen som på området strafferettslig håndheving (se betraktning 165–166).

3.3.2 *Videre bruk av de innsamlede opplysningene*

195) For behandling av personopplysninger som samles inn av sørkoreanske myndigheter for formål knyttet til nasjonal sikkerhet, gjelder prinsippene om formålsbegrensning (artikkel 3 nr. 1–2 i PIPA), lovlig og rettferdig behandling (artikkel 3 nr. 1 i PIPA), forholdsmessighet/dataminimering (artikkel 3 nr. 1 og 6 og artikkel 58 i PIPA), riktighet (artikkel 3 nr. 3 i PIPA), åpenhet (artikkel 3 nr. 5 i PIPA), sikkerhet (artikkel 58 nr. 4 i PIPA) og lagringsbegrensning (artikkel 58 nr. 4 i PIPA)([356]). En eventuell utlevering av personopplysninger til tredjeparter (herunder tredjeland) kan bare skje i samsvar med disse prinsippene (særlig om formålsbegrensning og dataminimering) etter at det er foretatt en vurdering av om prinsippene om nødvendighet og forholdsmessighet er overholdt (artikkel 37 nr. 2 i forfatningen), og idet det tas hensyn til hvilken innvirkning dette har på de berørte personenes rettigheter (artikkel 3 nr. 6 i PIPA).

196) Når det gjelder kommunikasjonsinnhold og kommunikasjonsbekreftelsesdata, begrenser CPPA bruken av slike opplysninger ytterligere til retterganger der en part i kommunikasjonen påberoper seg disse i et krav om skadeserstatning, eller til bruk som er tillatt i henhold til andre lover([357]).

3.3.3 *Tilsyn*

197) De sørkoreanske sikkerhetsmyndighetenes aktiviteter overvåkes av forskjellige organer([358]).

198) For det første inneholder antiterrorloven bestemmelser om spesifikke tilsynsmekanismer for terrorbekjempelsesaktiviteter, herunder innsamling av opplysninger om terrormistenkte. På det utøvende nivået overvåkes terrorbekjempelsesaktiviteter av antiterrorkommisjonen([359]), som direktøren for NIS skal rapportere til om etterforskning og sporing av terrormistenkte for å samle inn opplysninger eller materiale som er nødvendig for å bekjempe terrorisme([360]). Den ansvarlige for vern av menneskerettigheter (Human Rights Protection Officer – HRPO) fører dessuten spesifikt tilsyn med at terrorbekjempelsesaktivitetene ikke er i strid med grunnleggende rettigheter([361]). HRPO utnevnes av lederen for antiterrorkommisjonen blant personer som oppfyller spesifikke kvalifikasjonskriterier angitt i gjennomføringsdekretet til antiterrorloven([362]), for en (fornybar) periode på to år, og kan bare avsettes av spesifikke, begrensede grunner og dersom det er berettiget([363]). I utøvelsen av sin tilsynsfunksjon kan HRPO utstede generelle anbefalinger for å forbedre vernet

([354]) Artikkel 83 nr. 3 i TBA.
([355]) Se også vedlegg II avsnitt 3.2.3.
([356]) Se vedlegg II avsnitt 1.2.
([357]) Artikkel 5 nr.1–2, artikkel 12 og artikkel 13-5 i CPPA.
([358]) Se vedlegg II avsnitt 3.3.
([359]) Artikkel 5 nr. 3 i antiterrorloven. Kommisjonen ledes av statsministeren og består av flere ministere og ledere for statlige organer, for eksempel utenriksministeren, justisministeren, forsvarsministeren og innenriks- og sikkerhetsministeren, direktøren for NIS og generalkommissæren for den nasjonale politimyndigheten (artikkel 3 nr. 1 i gjennomføringsdekretet til antiterrorloven).
([360]) Artikkel 9 nr. 4 i antiterrorloven.
([361]) Artikkel 7 i antiterrorloven.
([362]) Det vil si enhver person med kvalifikasjoner som advokat og med minst ti års arbeidserfaring eller med ekspertkunnskap på området menneskerettigheter og som arbeider eller har arbeidet (minst) som assisterende professor i minst ti år, eller som har innehatt en stilling som høyere offentlig tjenestemann i statlige organer eller ved lokale myndigheter, eller med minst ti års arbeidserfaring på området menneskerettigheter, for eksempel i en ikke-statlig organisasjon (artikkel 7 nr. 1 i gjennomføringsdekretet til antiterrorloven).
([363]) For eksempel dersom det er reist tiltale i en straffesak knyttet til vedkommendes oppgaver, ved utlevering av konfidensielle opplysninger eller på grunn av langvarig svekket psykisk eller fysisk funksjonsevne (artikkel 7 nr. 3 i gjennomføringsdekretet til antiterrorloven).

av menneskerettighetene([364]) og spesifikke anbefalinger om korrigerende tiltak dersom det er konstatert at menneskerettighetene er blitt krenket([365]). De offentlige myndighetene skal underrette HRPO om oppfølgingen av disse anbefalingene([366]).

199) For det andre fører PIPC tilsyn med at de nasjonale sikkerhetsmyndighetene overholder reglene for vern av personopplysninger, som omfatter både de gjeldende bestemmelsene i PIPA (se betraktning 149) og begrensningene og garantiene som gjelder for innsamling av personopplysninger i henhold til andre lover (CPPA, antiterrorloven og TBA, se også betraktning 171)([367]). Ved utøvelsen av denne tilsynsrollen kan PIPC bruke all sin undersøkelsesmyndighet og korrigerende myndighet, som beskrevet nærmere i avsnitt 2.4.2.

200) For det tredje er de nasjonale sikkerhetsmyndighetenes aktiviteter underlagt NHRCs uavhengige tilsyn i samsvar med framgangsmåtene beskrevet i betraktning 172([368]).

201) For det fjerde omfatter BAIs tilsynsfunksjon også de nasjonale sikkerhetsmyndighetene, selv om NIS under ekstraordinære omstendigheter kan nekte å utlevere visse opplysninger eller materialer, for eksempel dersom de utgjør statshemmeligheter, og dersom det vil kunne ha alvorlige konsekvenser for den nasjonale sikkerheten dersom offentligheten får kjennskap til dem([369]).

202) For det femte utføres det parlamentariske tilsynet med NIS' aktiviteter av nasjonalforsamlingen (gjennom et spesialisert etterretningsutvalg)([370]). Nasjonalforsamlingens særlige tilsynsrolle når det gjelder bruken av kommunikasjonsbegrensende tiltak for formål knyttet til nasjonal sikkerhet, er fastsatt i CPPA([371]). Nasjonalforsamlingen kan særlig foreta stedlige inspeksjoner av avlyttingsutstyr og kreve at både NIS og teleoperatører som har utlevert kommunikasjonsinnhold, rapporterer om dette. Nasjonalforsamlingen kan også utøve sin generelle tilsynsfunksjon (i samsvar med framgangsmåtene beskrevet i betraktning 174). I henhold til NIS-loven skal direktøren for NIS reagere uten opphold når etterretningsutvalget anmoder om en rapport om en bestemt sak([372]), og det gjelder særlige regler for visse spesielt sensitive opplysninger. Direktøren for NIS kan bare nekte å svare eller avgi vitneforklaring for utvalget under ekstraordinære omstendigheter, det vil si dersom anmodningen gjelder statshemmeligheter om militære eller diplomatiske spørsmål eller spørsmål knyttet til Nord-Korea, og dersom det kan ha alvorlige konsekvenser for landets «nasjonale skjebne» dersom offentligheten får kjennskap til dette([373]). I slike tilfeller kan etterretningsutvalget anmode statsministeren om en forklaring, og dersom det ikke gis en forklaring innen sju dager, kan svaret eller vitneforklaringen ikke avslås.

3.3.4 *Prøvings- og klageadgang*

203) Også på området nasjonal sikkerhet er det i det sørkoreanske systemet en rekke forskjellige muligheter til å oppnå (rettslig) prøving, herunder mulighet til å oppnå skadeserstatning. Disse mekanismene gir de registrerte mulighet til effektiv administrativ og rettslige prøving, som særlig setter dem i stand til å gjøre sine rettigheter gjeldende, herunder retten til innsyn i egne personopplysninger eller til å få rettet eller slettet slike opplysninger.

204) For det første kan enkeltpersoner i henhold til artikkel 3 nr. 5 og artikkel 4 nr. 1, 3 og 4 i PIPA utøve sin rett til innsyn, retting, sletting og innstilling av behandlingen overfor nasjonale sikkerhetsmyndigheter. I melding 2021-5 avsnitt 6 (vedlegg I til denne beslutningen) presiseres det hvordan disse rettighetene får anvendelse i forbindelse med behandling

([364]) Artikkel 8 nr. 1 i gjennomføringsdekretet til antiterrorloven.

([365]) Artikkel 9 nr. 1 i gjennomføringsdekretet til antiterrorloven. HRPO treffer beslutning om vedtakelse av anbefalinger på en selvstendig måte, men skal rapportere slike anbefalinger til lederen for antiterrorkommisjonen.

([366]) Artikkel 9 nr. 2 i gjennomføringsdekretet til antiterrorloven. I henhold til den sørkoreanske regjeringens offisielle redegjørelser vil manglende gjennomføring av en anbefaling fra HRPO bli videresendt til antiterrorkommisjonen, herunder statsministeren, selv om det hittil ikke har vært tilfeller der HRPOs anbefalinger ikke er blitt gjennomført (se vedlegg II avsnitt 3.3.1).

([367]) Vedlegg II avsnitt 3.3.4.

([368]) Særlig når det gjelder NIS, har NHRC tidligere foretatt undersøkelser på eget initiativ og behandlet en rekke individuelle klager. Se for eksempel s. 128 i NHRCs årsrapport for 2018 (tilgjengelig på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) og s. 70 i NHRCs årsrapport for 2019 (tilgjengelig på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

([369]) Artikkel 13 nr. 1 i NIS-loven.

([370]) Artikkel 36 og 37 nr. 1 pkt. 15 i loven om nasjonalforsamlingen.

([371]) Artikkel 15 i CPPA.

([372]) Artikkel 15 nr. 2 i NIS-loven.

([373]) Artikkel 17 nr. 2 i NIS-loven. «Statshemmeligheter» defineres som (graderte) fakta, varer eller kunnskap som for å unngå alvorlige konsekvenser for den nasjonale sikkerheten ikke skal utleveres til andre land eller andre organisasjoner, og som det bare er begrenset tilgang til. Se artikkel 13 nr. 4 i NIS-loven.

av opplysninger for formål knyttet til nasjonal sikkerhet. En nasjonal sikkerhetsmyndighet kan bare begrense eller nekte utøvelsen av en slik rettighet i den grad og så lenge det er nødvendig og forholdsmessig for å beskytte et viktig mål av allmenn interesse (for eksempel i den grad og så lenge det å gi rettigheten vil bringe en pågående etterforskning i fare eller true den nasjonale sikkerheten), eller dersom det å gi rettigheten kan skade en tredjeparts liv eller legeme. Påberopelse av en slik begrensning krever derfor at den enkeltes rettigheter og interesser avveies mot den relevante allmenne interessen, og det må ikke under noen omstendigheter berøre rettighetens vesentlige innhold (artikkel 37 nr. 2 i forfatningen). Dersom anmodningen avslås eller begrenses, skal den aktuelle personen uten opphold underrettes om grunnene til dette.

205) For det andre har enkeltpersoner rett til å oppnå erstatning i henhold til PIPA dersom deres opplysninger er blitt behandlet av en nasjonal sikkerhetsmyndighet i strid med PIPA eller begrensningene og garantiene i andre lover om innsamling av personopplysninger (særlig CPPA, se betraktning 171)([374]). Denne rettigheten kan utøves ved å klage til PIPC (herunder via personverntelefontjenesten som drives av Republikken Koreas byrå for internett og sikkerhet)([375]). For å lette adgangen til å klage på sørkoreanske nasjonale sikkerhetsmyndigheter kan EU-borgere klage til PIPC via sin nasjonale personvernmyndighet([376]). Når undersøkelsen er avsluttet, vil PIPC da underrette den aktuelle personen via den nasjonale personvernmyndigheten (herunder, dersom det er relevant, med informasjon om de korrigerende tiltakene som er truffet). På grunnlag av forvaltningsprosessloven kan enkeltpersoner dessuten påklage/bestride PIPCs beslutninger eller unnlatelse av å handle (se betraktning 132).

206) For det tredje kan enkeltpersoner klage til HRPO angående krenking av deres rett til personvern / vern av personopplysninger i forbindelse med terrorbekjempelsesaktiviteter (det vil si i henhold til antiterrorloven)([377]), som kan anbefale korrigerende tiltak. Ettersom det ikke finnes noen formkrav til inngivelse av klager til HRPO, vil en klage bli behandlet selv om den aktuelle personen ikke kan bevise at vedkommende rent faktisk har lidd skade (for eksempel på grunn av en påstått ulovlig innsamling av vedkommendes opplysninger utført av en nasjonal sikkerhetsmyndighet)([378]). Den relevante myndigheten må underrette HRPO om alle tiltak som treffes for å gjennomføre HRPOs anbefalinger.

207) For det fjerde kan enkeltpersoner inngi en klage til NHRC angående de nasjonale sikkerhetsmyndighetenes innsamling av deres opplysninger og få prøvet saken i samsvar med framgangsmåten beskrevet i betraktning 178([379]).

208) For det femte finnes det forskjellige rettsmidler([380]) som gir enkeltpersoner mulighet til å påberope seg begrensningene og garantiene beskrevet i avsnitt 3.3.1 for å oppnå prøving. Enkeltpersoner kan framfor alt bestride lovligheten av nasjonale sikkerhetsmyndigheters handlinger på grunnlag av forvaltningsprosessloven (i samsvar med framgangsmåten beskrevet i betraktning 181 eller loven om forfatningsdomstolen (se betraktning 182)). De har dessuten mulighet til å oppnå erstatning på grunnlag av loven om statlig erstatning (som nærmere beskrevet i betraktning 183)).

4. KONKLUSJON

209) Kommisjonen anser at Republikken Korea – gjennom PIPA, de særlige reglene som gjelder for visse sektorer (som analysert i avsnitt 2), og de supplerende garantiene i melding 2021-5 (vedlegg I) – sikrer et beskyttelsesnivå for personopplysninger som overføres fra Den europeisk union, som i det vesentlige tilsvarer det som garanteres ved forordning (EU) 2016/679.

210) Kommisjonen mener videre at tilsyns- og prøvingsmekanismene i sørkoreansk rett i praksis gjør det mulig å identifisere og straffe overtredelser av reglene for vern av personopplysninger begått av behandlingsansvarlige i Republikken Korea, og at de sikrer at den registrerte har rettsmidler som gjør det mulig å få innsyn i egne personopplysninger og å få rettet eller slettet slike opplysninger.

([374]) Artikkel 58 nr. 4 og artikkel 4 nr. 5 i PIPA. Se vedlegg II avsnitt 3.4.2.
([375]) Artikkel 62 og artikkel 63 nr. 2 i PIPA.
([376]) Melding 2021-5 avsnitt 6 (vedlegg I).
([377]) Artikkel 8 nr. 1 pkt. 2 i gjennomføringsdekretet til antiterrorloven.
([378]) Se vedlegg II avsnitt 3.1.4.
([379]) NHRC mottar for eksempel regelmessig klager på den nasjonale etterretningstjenesten, se s. 70 i NHRCs årsrapport for 2019 for informasjon om antall mottatte klager mellom 2015 og 2019 (tilgjengelig på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Se vedlegg II avsnitt 3.4.4.

211) På grunnlag av den tilgjengelige informasjonen om den sørkoreanske rettsordenen, herunder redegjørelsene, forsikringene og de forpliktende tilsagnene fra den sørkoreanske regjeringen i vedlegg II, anser Kommisjonen at ethvert inngrep i allmennhetens interesse i de grunnleggende rettighetene til enkeltpersoner som får sine personopplysninger overført fra Den europeiske unionen til Republikken Korea, og som foretas av sørkoreanske myndigheter, særlig for formål knyttet til strafferettslig håndheving og nasjonal sikkerhet, vil være begrenset til det som er strengt nødvendig for å nå det aktuelle berettigede målet, og at det foreligger et effektivt rettslig vern mot slike inngrep.

212) I lys av resultatene i denne beslutningen bør det derfor besluttes at Republikken Korea sikrer et tilstrekkelig beskyttelsesnivå i betydningen angitt i artikkel 45 i forordning (EU) 2016/679, fortolket i lyset av Den europeiske unions pakt om grunnleggende rettigheter, for personopplysninger som overføres fra Den europeiske union til Republikken Korea til behandlingsansvarlige i Republikken Korea som omfattes av PIPA, med unntak av religiøse organisasjoners behandling av personopplysninger i forbindelse med misjonsvirksomhet, politiske partiers behandling av personopplysninger i forbindelse med nominering av kandidater og behandlingsansvarlige som er underlagt kommisjonen for finansielle tjenesters tilsyn med behandling av personlige kredittopplysninger i henhold til kredittopplysningsloven, i den grad de behandler slike opplysninger.

5. VIRKNINGER AV DENNE BESLUTNINGEN OG PERSONVERNMYNDIGHETENES TILTAK

213) Medlemsstatene og deres organer skal treffe de tiltakene som er nødvendige for å overholde EU-institusjonenes rettsakter, ettersom disse i prinsippet antas å være lovlige og dermed har rettsvirkning så lenge de ikke er trukket tilbake, opphevet innenfor rammen av en opphevingssak eller er erklært ugyldige som følge av en begjæring om forhåndsavgjørelse eller en påstand om rettsstridighet.

214) En kommisjonsbeslutning om tilstrekkelig beskyttelsesnivå truffet i henhold til artikkel 45 nr. 3 i forordning (EU) 2016/679 er derfor bindende for alle organer i medlemsstatene som den er rettet til, herunder deres uavhengige tilsynsmyndigheter. Overføringer fra en behandlingsansvarlig eller databehandler i Den europeiske union til behandlingsansvarlige i Republikken Korea kan derfor finne sted uten at det er nødvendig med ytterligere godkjenning.

215) Det bør bemerkes at det i henhold til artikkel 58 nr. 5 i forordning (EU) 2016/679 og som forklart av Den europeiske unions domstol i *Schrems*-dommen([381]) gjelder at dersom en personvernmyndighet reiser tvil om, herunder ved en klage, hvorvidt en kommisjonsbeslutning om tilstrekkelig beskyttelsesnivå er forenlig med en privatpersons grunnleggende rett til personvern og vern av personopplysninger, skal det i nasjonal rett foreligge rettsmidler som gjør det mulig å bringe nevnte klagepunkter inn for en nasjonal domstol, som kan være forpliktet til å framsette en begjæring om forhåndsavgjørelse for Den europeiske unions domstol([382]).

6. OVERVÅKING OG GJENNOMGÅELSE AV DENNE BESLUTNINGEN

216) I henhold til Domstolens rettspraksis([383]) og som anerkjent i artikkel 45 nr. 4 i forordning (EU) 2016/679 bør Kommisjonen fortløpende overvåke den relevante utviklingen i tredjelandet etter at en beslutning om tilstrekkelig beskyttelsesnivå er vedtatt, for å vurdere om tredjelandet fortsatt sikrer et i det vesentlige tilsvarende beskyttelsesnivå. En slik kontroll skal alltid foretas når Kommisjonen mottar informasjon som gir berettiget grunn til tvil om dette.

217) Kommisjonen bør derfor løpende overvåke situasjonen i Republikken Korea med hensyn til den rettslige rammen og faktisk praksis for behandling av personopplysninger som er vurdert i denne beslutningen, herunder de sørkoreanske myndighetenes overholdelse av redegjørelsene, garantiene og de forpliktende tilsagnene i vedlegg II. For å forenkle denne prosessen oppfordres de sørkoreanske myndighetene til straks å underrette Kommisjonen om vesentlige endringer som er relevante for denne beslutningen, med hensyn til økonomiske operatørers og offentlige myndigheters behandling av personopplysninger samt de begrensningene og garantiene som gjelder for offentlige myndigheters tilgang til personopplysninger.

([381]) *Schrems* nr. 65.

([382]) *Schrems* nr. 65: «Det påligger den nasjonale lovgiveren å fastsette rettsmidler som gjør det mulig for den aktuelle nasjonale tilsynsmyndigheten å bringe de klagepunktene den anser som velbegrunnede, inn for nasjonale domstoler, slik at de, dersom de deler myndighetens tvil vedrørende kommisjonsbeslutningens gyldighet, kan framsette en begjæring om forhåndsavgjørelse med henblikk på å undersøke beslutningens gyldighet.»

([383]) *Schrems* nr. 76.

218) For å gjøre det mulig for Kommisjonen å utøve sin overvåkingsfunksjon på en effektiv måte bør medlemsstatene underrette Kommisjonen om alle relevante tiltak truffet av nasjonale personvernmyndigheter, særlig med hensyn til henvendelser eller klager fra registrerte i EU om overføring av personopplysninger fra Den europeiske union til behandlingsansvarlige i Republikken Korea. Kommisjonen bør også underrettes om alle tegn på at tiltakene truffet av sørkoreanske offentlige myndigheter med ansvar for forebygging, etterforskning, avsløring eller straffeforfølging av straffbare forhold, eller for nasjonal sikkerhet, herunder eventuelle tilsynsorganer, ikke sikrer det nødvendige beskyttelsesnivået.

219) I henhold til artikkel 45 nr. 3 i forordning (EU) 2016/679([384]), og ettersom beskyttelsesnivået som den sørkoreanske rettsordenen sikrer, kan endres, bør Kommisjonen etter å ha truffet denne beslutningen regelmessig undersøke om konstateringen av at Republikken Korea sikrer et tilstrekkelig beskyttelsesnivå, fremdeles er saklig og rettslig begrunnet.

220) Med henblikk på dette bør en første gjennomgåelse av denne beslutningen foretas tre år etter at den er trådt i kraft. Etter denne første gjennomgåelsen og avhengig av utfallet vil Kommisjonen i nært samråd med komiteen nedsatt ved artikkel 93 nr. 1 i forordning (EU) 2016/679 beslutte om den treårige syklusen bør beholdes. I alle tilfeller bør etterfølgende gjennomgåelser finne sted minst hvert fjerde år([385]). Gjennomgåelsen bør omfatte alle aspekter av denne beslutningens virkemåte, særlig anvendelsen av de ytterligere garantiene i vedlegg I til denne beslutningen, med særlig oppmerksomhet rettet mot beskyttelsen som gis i tilfelle videreoverføring, relevant utvikling i rettspraksisen, reglene for behandling av pseudonymiserte opplysninger for statistiske formål og formål knyttet til vitenskapelig formål og arkivering i allmennhetens interesse samt anvendelsen av unntakene i artikkel 28 nr. 7 i PIPA, hvor effektiv utøvelsen av individuelle rettigheter er, herunder før den nylig reformerte PIPC, og anvendelsen av unntakene på disse rettighetene, anvendelsen av de delvise unntakene i henhold til PIPA samt begrensningene og garantiene som gjelder myndighetenes tilgang (som fastsatt i vedlegg II til denne beslutningen), herunder PIPCs samarbeid med personvernmyndigheter i EU om klager fra enkeltpersoner. Den bør også omfatte hvor effektivt tilsyn og håndheving er, både med hensyn til PIPA og på området strafferettslig håndheving og nasjonal sikkerhet (særlig i regi av PIPC og NHRC).

221) I forbindelse med gjennomgåelsen bør Kommisjonen ha møter med PIPC, eventuelt sammen med andre sørkoreanske myndigheter med ansvar for offentlige myndigheters tilgang, herunder relevante tilsynsorganer. Møtet bør være åpent for representanter for medlemmene av Det europeiske personvernråd. Innenfor rammen av gjennomgåelsen bør Kommisjonen anmode PIPC om å framlegge omfattende opplysninger om alle forhold som er relevante for konstateringen av at beskyttelsesnivået er tilstrekkelig, herunder begrensningene og garantiene som gjelder offentlige myndigheters tilgang([386]). Kommisjonen bør også be om forklaringer på eventuelle opplysninger den har mottatt som er relevante for denne beslutningen, herunder offentlige rapporter fra sørkoreanske myndigheter eller andre berørte parter i Republikken Korea, Det europeiske personvernråd, individuelle personvernmyndigheter, sivilsamfunnsgrupper, medierapporter eller andre tilgjengelige informasjonskilder.

222) Kommisjonen bør på grunnlag av gjennomgåelsen utarbeide en offentlig rapport som skal framlegges for Europaparlamentet og Rådet.

7. MIDLERTIDIG OPPHEVING, OPPHEVING ELLER ENDRING AV DENNE BESLUTNINGEN

223) Dersom tilgjengelig informasjon, særlig informasjon som stammer fra overvåkingen av denne beslutningen eller fra sørkoreanske eller medlemsstatenes myndigheter, viser at beskyttelsesnivået som Republikken Korea sikrer, kanskje ikke lenger er tilstrekkelig, bør Kommisjonen umiddelbart underrette vedkommende sørkoreanske myndigheter om dette og anmode om at det treffes egnede tiltak innen en fastsatt og rimelig frist.

224) Dersom vedkommende sørkoreanske myndigheter etter den angitte fristen ikke har truffet disse tiltakene eller på annen tilfredsstillende måte kan dokumentere at denne beslutningen fortsatt er basert på et tilstrekkelig beskyttelsesnivå, vil Kommisjonen i henhold til artikkel 93 nr. 2 i forordning (EU) 2016/679 innlede prosedyren med henblikk på delvis eller fullstendig midlertidig oppheving eller oppheving av denne beslutningen.

225) Alternativt vil Kommisjonen innlede den aktuelle prosedyren med henblikk på å endre beslutningen, særlig ved at overføring av opplysninger underlegges ytterligere vilkår, eller ved å begrense konstateringen av tilstrekkelig beskyttelsesnivå til bare å gjelde overføring av opplysninger der det fortsatt sikres et tilstrekkelig beskyttelsesnivå.

([384]) I henhold til artikkel 45 nr. 3 i forordning (EU) 2016/679 skal det i gjennomføringsrettsakten «[f]astsettes en mekanisme for regelmessig gjennomgåelse, […] der det skal tas hensyn til all relevant utvikling i tredjestaten eller den internasjonale organisasjonen».

([385]) I artikkel 45 nr. 3 i forordning (EU) 2016/679 er det fastsatt at det skal foretas regelmessig gjennomgåelse «minst hvert fjerde år». Se også Det europeiske personvernråd, Adequacy Referential, WP 254 rev. 01.

([386]) Se vedlegg II til denne beslutningen.

226) Kommisjonen bør særlig innlede prosedyren for midlertidig oppheving eller oppheving ved tegn på at de ytterligere garantiene angitt i vedlegg I ikke overholdes av økonomiske operatører som mottar personopplysninger i henhold til denne beslutningen, og/eller ikke håndheves effektivt, eller at de sørkoreanske myndighetene ikke etterlever redegjørelsene, garantiene og de forpliktende tilsagnene i vedlegg II til denne beslutningen.

227) Kommisjonen bør også vurdere å innlede prosedyren som fører til endring, midlertidig oppheving eller oppheving av denne beslutningen dersom vedkommende sørkoreanske myndigheter i forbindelse med gjennomgåelsen eller på annen måte unnlater å gi den informasjonen eller de presiseringene som er nødvendige for å vurdere beskyttelsesnivået for personopplysninger som overføres fra Den europeiske union til Republikken Korea, eller for å vurdere samsvaret med denne beslutningen. I denne forbindelse bør Kommisjonen ta hensyn til i hvilket omfang den relevante informasjonen kan innhentes fra andre kilder.

228) I behørig begrunnede tvingende hastetilfeller vil Kommisjonen benytte muligheten til, i henhold til framgangsmåten nevnt i artikkel 93 nr. 3 i forordning (EU) 2016/679, å vedta gjennomføringsrettsakter med umiddelbar virkning som midlertidig opphever, opphever eller endrer beslutningen.

8. AVSLUTTENDE BETRAKTNINGER

229) Det europeiske personvernråd har offentliggjort sin uttalelse([387]), og det er tatt hensyn til den ved utarbeidingen av denne beslutningen.

230) Tiltakene fastsatt i denne beslutningen er i samsvar med uttalelse fra komiteen nedsatt ved artikkel 93 i forordning (EU) 2016/679.

TRUFFET DENNE BESLUTNINGEN:

Artikkel 1

1. Med henblikk på artikkel 45 i forordning (EU) 2016/679 sikrer Republikken Korea et tilstrekkelig beskyttelsesnivå for personopplysninger som overføres fra Den europeiske union til enheter i Republikken Korea som omfattes av loven om vern av personopplysninger, supplert med de ytterligere garantiene fastsatt i vedlegg I, sammen med de offisielle redegjørelsene, forsikringene og forpliktende tilsagnene i vedlegg II.

2. Denne beslutningen omfatter ikke personopplysninger som overføres til mottakere som tilhører én av følgende kategorier, i den grad alle eller deler av formålene med behandlingen av personopplysningene svarer til ett av formålene angitt der:

a) Religiøse organisasjoners behandling av personopplysninger i forbindelse med sin misjonsvirksomhet.

b) Politiske partier i den grad de behandler personopplysninger i forbindelse med nominering av kandidater.

c) Enheter som er underlagt kommisjonen for finansielle tjenesters tilsyn med behandlingen av personlige kredittopplysninger i henhold til kredittopplysningsloven, i den grad de behandler slike opplysninger.

Artikkel 2

Dersom vedkommende myndigheter i medlemsstatene for å beskytte enkeltpersoner i forbindelse med behandling av deres personopplysninger utøver sin myndighet i henhold til artikkel 58 i forordning (EU) 2016/679 med hensyn til overføring av opplysninger som hører inn under virkeområdet fastsatt i artikkel 1 i denne beslutningen, skal den berørte medlemsstaten omgående underrette Kommisjonen.

Artikkel 3

1. Kommisjonen skal løpende overvåke anvendelsen av den rettslige rammen som denne beslutningen bygger på, herunder vilkårene for videreoverføring, utøvelsen av individuelle rettigheter og sørkoreanske offentlige myndigheters tilgang til opplysninger som overføres på grunnlag av denne beslutningen, med henblikk på å vurdere om Republikken Korea fortsatt sikrer et tilstrekkelig beskyttelsesnivå som definert i artikkel 1.

([387]) Uttalelse 32/2021 om Europakommisjonens utkast til gjennomføringsbeslutning i henhold til forordning (EU) 2016/679 om tilstrekkelig vern av personopplysninger i Republikken Korea (tilgjengelig på https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_en).

2. Medlemsstatene og Kommisjonen skal underrette hverandre om tilfeller der kommisjonen for vern av personopplysninger (PIPC) eller en annen vedkommende sørkoreansk myndighet ikke klarer å sikre samsvar med den rettslige rammen som denne beslutning bygger på.

3. Medlemsstatene og Kommisjonen skal underrette hverandre om ethvert tegn på at sørkoreanske offentlige myndigheter griper inn i den enkeltes rett til vern av egne personopplysninger utover det som er strengt nødvendig, eller på at det ikke foreligger et effektivt rettslig vern mot slike inngrep.

4. Senest tre år fra den datoen denne beslutningen er meddelt medlemsstatene og deretter minst hvert fjerde år skal Kommisjonen vurdere konklusjonene nevnt i artikkel 1 nr. 1 på grunnlag av all tilgjengelig informasjon, herunder informasjon mottatt som ledd i gjennomgåelsen som er utført sammen med de relevante sørkoreanske myndighetene.

5. Dersom Kommisjonen ser tegn på at et tilstrekkelig beskyttelsesnivå ikke lenger er sikret, skal Kommisjonen underrette vedkommende sørkoreanske myndigheter. Den kan om nødvendig beslutte å midlertidig oppheve, endre eller oppheve denne beslutningen eller begrense dens virkeområde i samsvar med artikkel 45 nr. 5 i forordning (EU) 2016/679, særlig ved tegn på at

a) behandlingsansvarlige i Republikken Korea som har mottatt personopplysninger fra Den europeiske union i henhold til denne beslutningen, ikke oppfyller de ytterligere garantiene i vedlegg I, eller at tilsynet med og håndhevingen av dette er utilstrekkelig,

b) sørkoreanske offentlige myndigheter ikke retter seg etter redegjørelsene, forsikringene og de forpliktende tilsagnene i vedlegg II, herunder vilkårene og begrensningene for sørkoreanske offentlige myndigheters innsamling av og tilgang til personopplysninger som er overført i henhold til denne beslutningen, for formål knyttet til strafferettslig håndheving eller nasjonal sikkerhet.

Kommisjonen kan også vedta slike tiltak dersom manglende samarbeid fra sørkoreanske myndigheter hindrer Kommisjonen i å fastslå om Republikken Korea fortsatt sikrer et tilstrekkelig beskyttelsesnivå.

Artikkel 4

Denne beslutningen er rettet til medlemsstatene.

Utferdiget i Brussel 17. desember 2021.

For Kommisjonen

Didier REYNDERS

Medlem av Kommisjonen

VEDLEGG I

UTFYLLENDE REGLER FOR FORTOLKNING OG ANVENDELSE AV LOVEN OM VERN AV PERSONOPPLYSNINGER I FORBINDELSE MED BEHANDLING AV PERSONOPPLYSNINGER SOM OVERFØRES TIL REPUBLIKKEN KOREA

Innhold

I. **Sammenfatning**

Republikken Korea og Den europeiske union (heretter kalt «EU») har hatt drøftinger om tilstrekkelig beskyttelsesnivå, og Europakommisjonen har i denne forbindelse fastslått at Republikken Korea sikrer et tilstrekkelig beskyttelsesnivå for personopplysninger i samsvar med artikkel 45 i GDPR.

I denne forbindelse vedtok kommisjonen for vern av personopplysninger (Personal Information Protection Commission – PIPC) denne meldingen på grunnlag av artikkel 5 (statens forpliktelser osv.) og artikkel 14 (internasjonalt samarbeid)([1]) i loven om vern av personopplysninger (Personal Information Protection Act – PIPA) for å presisere fortolkningen, anvendelsen og håndhevingen av visse bestemmelser i loven, herunder om behandling av personopplysninger som overføres til Republikken Korea på grunnlag av EUs beslutning om tilstrekkelig beskyttelsesnivå.

Ettersom denne meldingen har status som en forskrift som vedkommende forvaltningsorgan fastsetter og kunngjør for å presisere standardene for fortolkning, bruk og håndheving av loven om vern av personopplysninger i Republikken Koreas rettssystem, har den rettslig bindende virkning for den behandlingsansvarlige på den måten at enhver overtredelse av denne meldingen kan anses som en overtredelse av de relevante bestemmelsene i nevnte lov. Dersom personlige rettigheter og interesser krenkes som følge av en overtredelse av denne meldingen, har de berørte personene dessuten rett til å klage til kommisjonen for vern av personopplysninger eller domstolene.

Dersom den behandlingsansvarlige som behandler personopplysninger som er overført til Republikken Korea i henhold til EUs beslutning om tilstrekkelig beskyttelsesnivå, ikke treffer tiltak som er i samsvar med denne meldingen, vil det bli vurdert som at det er «vektige grunner til å anta at det har skjedd en overtredelse i forbindelse med personopplysninger, og at det dersom det ikke treffes tiltak, sannsynligvis vil forårsake skade som det er vanskelig å avhjelpe», i henhold til lovens artikkel 64 nr. 1 og 2.

([1]) I henhold til artikkel 14 i loven om vern av personopplysninger har den sørkoreanske regjeringen myndighet til å fastsette strategier for å forbedre beskyttelsesnivået for personopplysninger i det internasjonale miljøet og for å hindre at de registrertes rettigheter krenkes som følge av overføring over landegrensene av personopplysninger.

I slike tilfeller kan kommisjonen for vern av personopplysninger eller tilknyttede sentrale forvaltningsorganer pålegge den relevante behandlingsansvarlige å treffe korrigerende tiltak osv. i henhold til den myndigheten som gis i denne bestemmelsen, og avhengig av de spesifikke lovovertredelsene kan det også ilegges tilsvarende straff (sanksjoner, overtredelsesgebyrer osv.).

II. **Definisjoner**

I denne teksten menes med

i) «lov» loven om vern av personopplysninger (lov nr. 16930 endret 4. februar 2020 og trådt i kraft 5. august 2020),

ii) «presidentdekret» gjennomføringsdekret til loven om vern av personopplysninger (presidentdekret nr. 30509 av 3. mars 2020, endrer andre lover),

iii) «registrert» en person som kan identifiseres ved hjelp av opplysningene som behandles, og som opplysningene dermed gjelder,

iv) «behandlingsansvarlig» en offentlig institusjon, juridisk person, organisasjon, enkeltperson osv. som behandler personopplysninger direkte eller indirekte som en del av sin virksomhet,

v) «EU» EU (ved utgangen av februar 2020 var det 27 medlemsstater([2]), herunder Belgia, Tyskland, Frankrike, Italia, Luxemburg, Nederland, Danmark, Irland, Hellas, Portugal, Spania, Østerrike, Finland, Sverige, Kypros, Tsjekkia, Estland, Ungarn, Latvia, Litauen, Malta, Polen, Slovakia, Slovenia, Romania, Bulgaria og Kroatia) og stater som er assosiert med EU gjennom EØS-avtalen (Island, Liechtenstein og Norge),

vi) «GDPR» EUs generelle regelverk for vern av personopplysninger, den generelle personvernforordningen (forordning (EU) 2016/679),

vii) «beslutning om tilstrekkelig beskyttelsesnivå» – i henhold til artikkel 45 nr. 3 i GDPR kan Europakommisjonen beslutte at et tredjeland, et territorium i et tredjeland, et eller flere områder eller en internasjonal organisasjon sikrer et tilstrekkelig beskyttelsesnivå for personopplysninger.

III. **Utfyllende regler**

1. **Begrensning av ikke-formålsmessig bruk og videreformidling av personopplysninger (lovens artikkel 3, 15 og 18)**

<Loven om vern av personopplysninger

(lov nr. 16930, delvis endret 4. februar 2020)>

Artikkel 3 (prinsipper for vern av personopplysninger) 1. Den behandlingsansvarlige skal uttrykkelig angi formålene som personopplysninger behandles for, og skal samle inn personopplysninger på en lovlig og rettferdig måte i så lite omfang som nødvendig for å oppfylle disse formålene.

2. Den behandlingsansvarlige skal behandle personopplysninger på en måte som er egnet og nødvendig for formålene som personopplysningene behandles for, og skal ikke bruke dem for andre formål.

Artikkel 15 (innsamling og bruk av personopplysninger) 1. En behandlingsansvarlig kan samle inn personopplysninger i følgende tilfeller og bruke dem innenfor rammen av formålet med innsamlingen:

1. Dersom det er innhentet samtykke fra en registrert.

2. Dersom det finnes særlige bestemmelser i lovgivningen, eller dersom det kreves for å overholde rettslige forpliktelser.

3. Dersom det kreves for at en offentlig institusjon skal kunne ivareta de oppgavene som hører inn under dens kompetanse i henhold til lovgivningen, osv.

4. Dersom det er et obligatorisk krav for å gjennomføre og oppfylle en avtale med en registrert.

([2]) Fram til utløpet av overgangsperioden omfatter dette også Det forente kongerike som fastsatt i artikkel 126, 127 og 132 i avtalen om Det forente kongerike Storbritannia og Nord-Irlands utmelding av Den europeiske union og Det europeiske atomenergifellesskap (2019/C 384 I/01).

5. Dersom det anses for å være åpenbart nødvendig for å beskytte den registrertes eller en tredjeparts liv, legeme eller eiendomsinteresser mot overhengende fare, dersom den registrerte eller vedkommendes rettslige representant ikke er i stand til å uttrykke sin mening, eller dersom det ikke er mulig å innhentes samtykke på forhånd på grunn av ukjent adresse, osv.

6. Dersom det er nødvendig for å beskytte en behandlingsansvarligs rettmessige interesse, dersom denne interessen klart går foran den registrertes rettigheter. I slike tilfeller er behandling bare tillatt dersom den i vesentlig grad er knyttet til den behandlingsansvarliges berettigede interesse og holdes innenfor et rimelig omfang.

Artikkel 18 (begrensning av ikke-formålsmessig bruk og videreformidling av personopplysninger) 1. En behandlingsansvarlig skal ikke bruke personopplysninger utenfor rammen av virkeområdet fastsatt i artikkel 15 nr. 1 og artikkel 39-3 nr. 1 og 2 eller videreformidle dem til en tredjepart utenfor rammene av virkeområdet fastsatt i artikkel 17 nr. 1 og 3.

2. Uten hensyn til nr. 1 kan en behandlingsansvarlig, dersom noen av punktene nedenfor får anvendelse, bruke personopplysninger eller videreformidle dem til en tredjepart for andre formål, med mindre det er sannsynlig at det vil krenke den registrertes eller tredjepartens interesse urettmessig: Leverandører av informasjons- og kommunikasjonstjenester [som fastsatt i artikkel 2 nr. 1 pkt. 3 i loven om fremming av bruken av informasjons- og kommunikasjonsnettverk og vern av opplysninger osv., heretter gjelder det samme] som behandler personopplysninger om brukere [som fastsatt i artikkel 2 nr. 1 pkt. 4 i loven om fremming av bruken av informasjons- og kommunikasjonsnettverk og vern av opplysninger osv., heretter gjelder det samme] omfattes bare av nr. 1 og 2, og nr. 5–9 får bare anvendelse på offentlige institusjoner

1. dersom det er innhentet ytterligere samtykke fra den registrerte,

2. dersom det finnes andre særlige bestemmelser i lovgivningen,

3. dersom det anses for å være åpenbart nødvendig for å beskytte den registrertes eller en tredjeparts liv, legeme eller eiendomsinteresser mot overhengende fare, dersom den registrerte eller vedkommendes rettslige representant ikke er i stand til å uttrykke sin mening, eller dersom det ikke er mulig å innhentes samtykke på forhånd på grunn av ukjent adresse,

4. slettet <ved lov nr. 16930 av 4. feb. 2020>

5. dersom det er umulig å utføre oppgavene som hører inn under vedkommendes kompetanse i henhold til lovgivningen, med mindre den behandlingsansvarlige bruker personopplysninger for andre formål enn det tiltenkte formålet, eller videreformidler dem til en tredjepart, og er underlagt kommisjonens behandling av spørsmålet og beslutning om dette,

6. dersom det er nødvendig å videreformidle personopplysninger til en utenlandsk regjering eller internasjonal organisasjon for å gjennomføre en traktat eller en annen internasjonal konvensjon,

7. dersom det er nødvendig for å etterforske og rettsforfølge straffbare forhold eller for å reise tiltale,

8. dersom det er nødvendig for at en domstol skal kunne utføre rettsaksrelaterte oppgaver,

9. dersom det er nødvendig med henblikk på iverksetting av straff, prøveløslatelse og varetektsfengsling.

Nr. 3 og 4 utelatt.

5. Dersom en behandlingsansvarlig videreformidler personopplysninger til en tredjepart for andre formål enn det tiltenkte i situasjonene omhandlet i nr. 2, skal den behandlingsansvarlige anmode mottakeren av personopplysningene om å begrense formålet med og metoden for bruk og andre nødvendige elementer, eller om å utarbeide nødvendige garantier for å garantere personopplysningenes sikkerhet. I slike tilfeller skal personen som mottar en slik anmodning, treffe de nødvendige tiltakene for å garantere personopplysningenes sikkerhet.

i) I lovens artikkel 3 nr. 1 og 2 fastsettes prinsippet om at en behandlingsansvarlig bare må samle inn den minste mengden personopplysninger som kreves for å oppfylle formålet med behandlingen av personopplysninger på lovlig vis, og ikke skal bruke dem for andre formål enn det tiltenkte([3]).

ii) I henhold til dette prinsippet er det i lovens artikkel 15 nr. 1 fastsatt at når en behandlingsansvarlig samler inn personopplysninger, kan personopplysningene brukes innenfor rammen av formålet med innsamlingen, og i artikkel 18 nr. 1 er det fastsatt at personopplysninger ikke skal brukes til noe annet enn det tiltenkte formålet eller videreformidles til en tredjepart.

([3]) Ettersom disse bestemmelsene inneholder generelle prinsipper som gjelder for enhver behandling av personopplysninger, herunder dersom slik behandling spesifikt reguleres i andre lover, gjelder presiseringene i dette avsnittet også dersom personopplysninger behandles på grunnlag av andre lover (se for eksempel artikkel 15 nr. 1 i kredittopplysningsloven, der det henvises spesifikt til disse bestemmelsene).

iii) Selv om personopplysninger kan brukes for andre formål enn det tiltenkte eller videreformidles til en tredjepart i unntakstilfellene([4]) beskrevet i lovens artikkel 18 nr. 2, skal det stilles krav om at formålet eller metoden for bruk begrenses, slik at personopplysningene kan behandles på en sikker måte i henhold til nr. 5, eller at det treffes tiltak for å garantere personopplysningenes sikkerhet.

iv) Bestemmelsene nevnt over får tilsvarende anvendelse på behandling av alle personopplysninger som mottas innenfor Republikken Koreas rettslige jurisdiksjon fra et tredjeland, uavhengig av den registrertes nasjonalitet.

v) Dersom en behandlingsansvarlig i EU for eksempel overfører personopplysninger til en sørkoreansk behandlingsansvarlig i henhold til Europakommisjonens beslutning om tilstrekkelig beskyttelsesnivå, skal formålet med overføringen av personopplysningene fra den behandlingsansvarlige i EU anses som den sørkoreanske behandlingsansvarliges formål med innsamling av personopplysninger, og i slike tilfeller kan den sørkoreanske behandlingsansvarlige bare bruke personopplysningene eller videreformidle dem til en tredjepart innenfor rammen av formålet med innsamlingen, bortsett fra i unntakstilfellene beskrevet i lovens artikkel 18 nr. 2.

2. **Begrensning av videreoverføring av personopplysninger (lovens artikkel 17 nr. 3 og 4 og artikkel 18)**

<Loven om vern av personopplysninger

(lov nr. 16930, delvis endret 4. februar 2020)>

Artikkel 17 (videreformidling av personopplysninger) 1. Utelatt.

2. En behandlingsansvarlig skal underrette en registrert om følgende forhold i forbindelse med innhentingen av samtykke i henhold til nr. 1 pkt. 1. Det samme gjelder når noe av det følgende endres:

1. Mottakeren av personopplysningene.
2. Formålet som mottakeren av personopplysningene bruker slike opplysninger for.
3. Elementer i personopplysningene som skal videreformidles.
4. Perioden der mottakeren oppbevarer og bruker personopplysningene.
5. Det faktum at den registrerte har rett til å nekte å gi sitt samtykke og eventuelle ulemper som følger av det.

3. En behandlingsansvarlig skal underrette en registrert om forholdene fastsatt i nr. 2 og innhente samtykke fra den registrerte for å videreformidle personopplysninger til en tredjepart i utlandet, og skal ikke inngå en avtale om overføring over landegrensene av personopplysninger i strid med denne loven.

4. En behandlingsansvarlig kan videreformidle personopplysninger uten den registrertes samtykke innenfor rammer som er rimelig relatert til formålene som personopplysningene opprinnelig ble samlet inn for, i samsvar med elementer fastsatt ved presidentdekret, idet det tas hensyn til eventuelle ulemper for den registrerte og om nødvendige sikkerhetstiltak, for eksempel kryptering, er truffet, osv.

※ Se side 3, 4 og 5 angående artikkel 18.

<**Gjennomføringsdekret til loven om vern av personopplysninger** ([dato for gjennomføring: 5. februar 2021.]

[Presidentdekret nr. 30892 av 4. august 2020, endrer andre lover])>

Artikkel 14-2 (standarder for videre bruk/videreformidling av personopplysninger osv.)

1. Dersom en behandlingsansvarlig bruker eller videreformidler personopplysninger (heretter kalt «videre bruk eller videreformidling av personopplysninger») uten den registrertes samtykke i samsvar med lovens artikkel 15 nr. 3 eller artikkel 17 nr. 4, skal den behandlingsansvarlige ta hensyn til det følgende:

1. Om dette er rimelig relatert til det opprinnelige formålet som personopplysningene ble samlet inn for.
2. Om videre bruk eller videreformidling av personopplysningene kan forventes i lys av omstendighetene som personopplysningene ble samlet inn under, samt behandlingspraksis.
3. Om videre bruk eller videreformidling av personopplysningene ikke krenker den registrertes interesser urettmessig.
4. Om de nødvendige tiltakene for å garantere sikkerheten, for eksempel pseudonymisering eller kryptering, er truffet.

([4]) Leverandører av informasjons- og kommunikasjonstjenester omfattes bare av artikkel 18 nr. 2 pkt. 1 og 2. Pkt. 5–9 får bare anvendelse på offentlige institusjoner.

2. Den behandlingsansvarlige skal på forhånd offentliggjøre kriteriene for vurdering av punktene nevnt i nr. 1 i personvernprogrammet fastsatt i henhold til lovens artikkel 30 nr. 1, og den personvernansvarlige i henhold til lovens artikkel 31 nr. 1 skal kontrollere om den behandlingsansvarlige bruker eller videreformidler ytterligere personopplysninger i samsvar med de relevante standardene.

i. Dersom den behandlingsansvarlige videreformidler personopplysninger til en tredjepart i utlandet, må vedkommende på forhånd underrette de registrerte om alle elementene beskrevet i lovens artikkel 17 nr. 2 og innhente deres samtykke, unntatt i tilfeller som omfattes av nr. 1 eller 2. Det skal ikke inngås avtaler om videreformidling over landegrensene av personopplysninger i strid med denne loven.

   1) Dersom personopplysninger videreformidles innenfor rammer som er rimelig relatert til det opprinnelige formålet med innsamlingen, i henhold til lovens artikkel 17 nr. 4. De tilfellene der denne bestemmelsen kan anvendes, er imidlertid begrenset til tilfeller der standardene for videre bruk og videreformidling av personopplysninger fastsatt i artikkel 14-2 i gjennomføringsdekretet er oppfylt. Den behandlingsansvarlige skal dessuten vurdere om videreformidlingen av personopplysningene kan være til ulempe for de registrerte, og om vedkommende har truffet de tiltakene som er nødvendige for å garantere sikkerheten, for eksempel kryptering.

   2) Dersom personopplysninger kan videreformidles til en tredjepart i unntakstilfellene nevnt i lovens artikkel 18 nr. 2 (se s. 3 ~ 5). Også i slike tilfeller kan personopplysningene imidlertid ikke videreformidles til en tredjepart dersom det er sannsynlig at videreformidlingen av slike personopplysninger vil krenke den registrertes eller en tredjeparts interesser urettmessig. Den som videreformidler personopplysningene, skal dessuten be mottakeren av personopplysningene om å begrense formålet eller metoden for bruk av personopplysningene eller treffe de tiltakene som er nødvendige for å garantere personopplysningenes sikkerhet, slik at de kan behandles på en sikker måte.

ii. Dersom personopplysninger videreformidles til en tredjepart i utlandet, er det ikke sikkert at de vil bli omfattet av det beskyttelsesnivået som garanteres i den sørkoreanske loven om vern av personopplysninger, i og med at systemene for vern av personopplysninger varierer fra land til land. Slike tilfeller vil derfor bli ansett som «tilfeller som kan føre til ulemper for den registrerte» nevnt i lovens artikkel 17 nr. 4, eller «tilfeller der den registrertes eller en tredjeparts interesser krenkes urettmessig» nevnt i lovens artikkel 18 nr. 2 og i artikkel 14-2 i gjennomføringsdekretet til samme lov([5]). For å oppfylle kravene i disse bestemmelsene skal den behandlingsansvarlige og tredjeparten derfor uttrykkelig sikre et beskyttelsesnivå som tilsvarer det som er fastsatt i loven, herunder garantere at den registrerte kan utøve sine rettigheter i rettslig bindende dokumenter, for eksempel avtaler, også etter at personopplysningene er overført til utlandet.

3. **Underretning om opplysningene dersom personopplysningene ikke er samlet inn fra den registrerte (lovens artikkel 20)**

<Loven om vern av personopplysninger

(lov nr. 16930, delvis endret 4. februar 2020)>

Artikkel 20 (underretning om kilder osv. til personopplysninger samlet inn fra tredjeparter) 1. Når en behandlingsansvarlig behandler personopplysninger som er samlet inn fra tredjeparter, skal den behandlingsansvarlige umiddelbart underrette den registrerte om følgende forhold på dennes anmodning:

1. Kilden til de innsamlede personopplysningene.

2. Formålet med behandlingen av personopplysninger.

3. Det faktum at den registrerte har rett til å kreve at behandlingen av personopplysninger innstilles, som fastsatt i artikkel 37.

2. Uten at det berører nr. 1, skal en behandlingsansvarlig som oppfyller kriteriene fastsatt ved presidentdekret, idet det tas hensyn til typen og mengden behandlede personopplysninger, antall ansatte, salgsbeløp osv., og samler inn personopplysninger fra tredjeparter og behandler dem i henhold til artikkel 17 nr. 1 pkt. 1, underrette den registrerte om forholdene nevnt i nr. 1. Dette gjelder imidlertid ikke dersom opplysningene som samles inn av den behandlingsansvarlige, ikke inneholder personopplysninger, for eksempel kontaktopplysninger, som kan brukes til å underrette den registrerte.

([5]) I henhold til artikkel 18 nr. 2 pkt. 2 i PIPA gjelder dette også når personopplysninger utleveres til tredjeparter i utlandet på grunnlag av bestemmelser i andre lover (for eksempel kredittopplysningsloven).

3. Nødvendige elementer angående frist, metode og framgangsmåte for underretning av den registrerte i henhold til hovedbestemmelsen i nr. 2 skal fastsettes ved presidentdekret.

4. Nr. 1 og hovedklausulen i nr. 2 får ikke anvendelse i tilfellene nedenfor. Dette gjelder imidlertid bare når dette klart går foran de registrertes rettigheter i henhold til denne loven:

1. Dersom personopplysninger som er gjenstand for en anmodning om underretning, inngår i personopplysningsfilene nevnt i et av punktene i artikkel 32 nr. 2.
2. Dersom det er sannsynlig at en slik underretning vil forårsake skade på en annen persons liv eller legeme eller urettmessig vil skade en annen persons eiendom og andre interesser.

i) Dersom den behandlingsansvarlige mottar personopplysninger som er overført fra EU på grunnlag av EUs beslutning om tilstrekkelig beskyttelsesnivå([6]), skal vedkommende uten unødig opphold og under alle omstendigheter senest en måned etter overføringen gi den registrerte informasjonen i nr. 1–5 nedenfor.

1) Navn på og kontaktopplysninger til personene som overfører og mottar personopplysningene.

2) De opplysningene eller kategoriene av personopplysninger som overføres.

3) Formålet med innsamlingen og bruken av personopplysningene (som fastsatt av dataeksportøren i henhold til nr. 1 i denne meldingen).

4) Hvor lenge personopplysningene lagres.

5) Informasjon om den registrertes rettigheter i forbindelse med behandlingen av personopplysninger, metoden og framgangsmåten for å utøve rettighetene og eventuelle ulemper som utøvelsen av rettighetene kan medføre.

ii) Dersom den behandlingsansvarlige videreformidler personopplysningene i punkt i) til en tredjepart i Republikken Korea eller utlandet, skal vedkommende også gi den registrerte informasjonen i nr. 1–5 før personopplysningene videreformidles.

1) Navn på og kontaktopplysninger til personene som videreformidler og mottar personopplysningene.

2) De opplysningene eller kategoriene av personopplysninger som videreformidles.

3) Landet som personopplysningene skal videreformidles til, den planlagte datoen og metoden for videreformidling (begrenset til tilfeller der personopplysninger skal videreformidles til en tredjepart i utlandet).

4) Videreformidlerens formål med og rettslige grunnlag for videreformidlingen av personopplysningene.

5) Informasjon om den registrertes rettigheter i forbindelse med behandlingen av personopplysninger, metoden og framgangsmåten for å utøve rettighetene og eventuelle ulemper som utøvelsen av disse kan medføre.

iii) Den behandlingsansvarlige kan ikke anvende punkt i) eller ii) i tilfellene nevnt i nr. 1–4.

1) Dersom personopplysningene som det skal gis underretning om, inngår i en av følgende personopplysningsfiler nevnt i lovens artikkel 32 nr. 2, i den grad interessene som beskyttes ved denne bestemmelsen, klart går foran den registrertes rettigheter, og bare så lenge underretningen vil true de berørte interessene, for eksempel bringe en pågående strafferettslig etterforskning i fare eller true den nasjonale sikkerheten.

2) Dersom og så lenge det er sannsynlig at underretningen kan skade en annen persons liv eller legeme, eller urettmessig krenke en annen persons eiendomsinteresser, dersom disse rettighetene eller interessene klart går foran den registrertes rettigheter.

3) Dersom den registrerte allerede har informasjonen som den behandlingsansvarlige skal gi i samsvar med punkt i) eller ii).

4) Dersom den behandlingsansvarlige ikke har den registrertes kontaktopplysninger, eller dersom det innebærer en uforholdsmessig stor innsats å kontakte den registrerte, herunder i forbindelse med behandling på vilkårene angitt i avsnitt 3 i loven om vern av personopplysninger. Ved vurderingen av om det er mulig å kontakte den registrerte, eller om dette innebærer en uforholdsmessig stor innsats, skal muligheten for å samarbeide med dataeksportøren i EU tas i betraktning.

([6]) Forpliktelsene i punkt i), ii) og iii) får tilsvarende anvendelse når den behandlingsansvarlige som mottar personopplysninger fra EU på grunnlag av beslutningen om tilstrekkelig beskyttelsesnivå, behandler slike opplysninger på grunnlag av andre lover, for eksempel kredittopplysningsloven.

4. **Virkeområde for det særlige unntaket for behandling av pseudonymiserte opplysninger (lovens artikkel 28-2, 28-3, 28-4, 28-5, 28-6 og 28-7, artikkel 3 og artikkel 58-2)**

<Loven om vern av personopplysninger

(lov nr. 16930, delvis endret 4. februar 2020)>

Kapittel III Behandling av personopplysninger

AVSNITT 3 Særlige tilfeller som gjelder pseudonymiserte opplysninger

Artikkel 28-2 (behandling av pseudonymiserte opplysninger) 1. En behandlingsansvarlig kan behandle pseudonymiserte opplysninger uten den registrertes samtykke for statistiske formål og formål knyttet til vitenskapelig forskning og arkivering i allmennhetens interesse osv.

2. En behandlingsansvarlig skal ikke ta med opplysninger som kan brukes til å identifisere en bestemt person, ved videreformidling av pseudonymiserte opplysninger til en tredjepart i henhold til nr. 1.

Artikkel 28-3 (begrensning av samkjøring av pseudonymiserte opplysninger) 1. Uten at det berører artikkel 28-2, skal samkjøringen av pseudonymiserte opplysninger som behandles av forskjellige behandlingsansvarlige for statistiske formål og formål knyttet til vitenskapelig forskning og arkivering i allmennhetens interesse osv., foretas av en spesialisert institusjon utpekt av PIPC eller lederen for det tilknyttede sentrale forvaltningsorganet.

2. En behandlingsansvarlig som akter å utlevere de samkjørte opplysningene utenfor organisasjonen som har samkjørt opplysningene, skal innhente godkjenning fra lederen for den spesialiserte institusjonen etter å ha pseudonymisert opplysningene eller omgjort dem til formatet nevnt i artikkel 58-2.

3. Nødvendige elementer, herunder framgangsmåten og metodene for samkjøring i henhold til nr. 1, standarder og framgangsmåter for utpeking eller tilbakekalling av utpekingen av ledelsen for og tilsynet med en spesialisert institusjon, og standarder og framgangsmåter for eksport og godkjenning i henhold til nr. 2 skal fastsettes ved presidentdekret.

Artikkel 28-4 (plikt til å treffe sikkerhetstiltak i forbindelse med pseudonymiserte opplysninger) 1. Ved behandling av pseudonymiserte opplysninger skal en behandlingsansvarlig treffe de tekniske, organisatoriske og fysiske tiltakene, herunder atskilt lagring og forvaltning av ytterligere opplysninger som er nødvendige for å gjenopprette opplysningenes opprinnelige form, som kan være nødvendige for å garantere sikkerheten som fastsatt ved presidentdekret, slik at personopplysningene ikke går tapt, stjeles, utleveres, forfalskes, endres eller skades.

2. En behandlingsansvarlig som akter å behandle pseudonymiserte opplysninger, skal utarbeide og føre registre over elementer fastsatt ved presidentdekret, herunder formålet med behandlingen av de pseudonymiserte opplysningene og om tredjepartsmottakeren når pseudonymiserte opplysninger videreformidles, med henblikk på å forvalte behandlingen av pseudonymiserte opplysninger.

Artikkel 28-5 (forbudte handlinger i forbindelse med behandling av pseudonymiserte opplysninger) 1. Ingen skal behandle de pseudonymiserte opplysningene med det formålet å identifisere en bestemt person.

2. Dersom det under behandlingen av de pseudonymiserte opplysningene genereres opplysninger som identifiserer en bestemt person, skal den behandlingsansvarlige umiddelbart avbryte behandlingen og hente ut og tilintetgjøre opplysningene.

Artikkel 28-6 (ilegging av administrative tilleggsgebyrer for behandling av pseudonymiserte opplysninger) 1. Kommisjonen kan ilegge behandlingsansvarlige som har behandlet opplysninger for det formålet å identifisere en bestemt person i strid med artikkel 28-5 nr. 1, en bot som tilsvarer høyst tre hundredeler av det samlede salget. Dersom det ikke forekommer salg eller det er vanskelig å beregne salgsinntektene, kan den behandlingsansvarlige ilegges en bot på høyst KRW 400 millioner eller tre hundredeler av kapitalbeløpet, alt etter hvilket beløp som er høyest.

2. Artikkel 34-2 nr. 3–5 gjelder tilsvarende med nødvendige endringer for elementer som er nødvendige for å innføre og innkreve administrative tilleggsgebyrer.

Artikkel 28-7 (virkeområde) Artikkel 20, 21 og 27, artikkel 34 nr. 1 og artikkel 35–37, 39-3, 39-4 og 39-6–39-8 får ikke anvendelse på pseudonymiserte opplysninger.

Kapittel I Generelle bestemmelser

Artikkel 3 (prinsipper for vern av personopplysninger) 1. Den behandlingsansvarlige skal uttrykkelig angi formålene som personopplysninger behandles for, og skal samle inn personopplysninger på en lovlig og rettferdig måte i så lite omfang som nødvendig for å oppfylle disse formålene.

2. Den behandlingsansvarlige skal behandle personopplysninger på en måte som er egnet og nødvendig for formålene som personopplysningene behandles for, og skal ikke bruke dem for andre formål.

3. Den behandlingsansvarlige skal sikre at personopplysningene er riktige, fullstendige og oppdaterte i det omfanget som er nødvendig for formålene som personopplysningene behandles for.

4. Den behandlingsansvarlige skal håndtere personopplysninger på en sikker måte i henhold til behandlingsmetodene for og typene av osv. personopplysninger, idet det tas hensyn til risikoen for å krenke den registrertes rettigheter og hvor alvorlig den relevante risikoen er.

5. Den behandlingsansvarlige skal offentliggjøre sitt personvernprogram og andre elementer knyttet til behandlingen av personopplysninger og skal garantere den registrertes rettigheter, for eksempel retten til innsyn i egne personopplysninger.

6. Den behandlingsansvarlige skal behandle personopplysninger på en måte som minimerer muligheten for å krenke en registrerts personvern.

7. Dersom det fortsatt er mulig å oppfylle formålet med innsamlingen av personopplysninger ved å behandle anonymiserte eller pseudonymiserte personopplysninger, skal den behandlingsansvarlige bestrebe seg på å behandle personopplysninger gjennom anonymisering dersom anonymisering er mulig, eller gjennom pseudonymisering dersom det ikke er mulig å oppfylle formålet med innsamlingen av personopplysninger gjennom anonymisering.

8. Den behandlingsansvarlige skal bestrebe seg på å vinne de registrertes tillit ved å overholde og utføre oppgavene og ansvaret fastsatt i denne loven og i andre relaterte lover.

Kapittel IX Tilleggsbestemmelser

Artikkel 58-2 (unntak fra anvendelse) Denne loven får ikke anvendelse på opplysninger som ikke lenger identifiserer en bestemt person når de samkjøres med andre opplysninger, idet det tas rimelig hensyn til tid, kostnad, teknologi osv. <Denne artikkelen er nylig innsatt ved lov nr. 16930 av 4. februar 2020>

i. I henhold til kapittel III avsnitt 3 om særlige tilfeller som gjelder pseudonymiserte opplysninger (artikkel 28-2–28-7) tillates behandling av pseudonymiserte opplysninger uten den registrertes samtykke for statistiske formål og formål knyttet til vitenskapelig forskning og oppbevaring av offentlige registre osv. (artikkel 28-2), men i slike tilfeller kreves det egnede garantier og forbud for å verne de registrertes rettigheter (artikkel 28-4 og 28-5), det kan ilegges tilleggssanksjoner for overtredelser (artikkel 28-6) og visse garantier som ellers er tilgjengelige i henhold til PIPA, får ikke anvendelse (artikkel 28-7).

ii. Disse bestemmelsene får ikke anvendelse i tilfeller der pseudonymiserte opplysninger behandles for andre formål enn statistiske formål og formål knyttet til vitenskapelig forskning og oppbevaring av offentlige registre osv. Dersom en EU-borgers personopplysninger som er overført til Republikken Korea i henhold til Europakommisjonens beslutning om tilstrekkelig beskyttelsesnivå, pseudonymiseres for andre formål enn statistiske formål og formål knyttet til vitenskapelig forskning og oppbevaring av offentlige registre osv., får de særlige bestemmelsene i kapittel III avsnitt 3 for eksempel ikke anvendelse([7]).

iii. Dersom en behandlingsansvarlig behandler pseudonymiserte opplysninger for statistiske formål og formål knyttet til vitenskapelig forskning og oppbevaring av offentlige registre osv., og dersom de pseudonymiserte opplysningene ikke er blitt tilintetgjort når det spesifikke formålet med behandlingen er oppfylt i samsvar med forfatningens artikkel 37 og lovens artikkel 3 (prinsipper for vern av personopplysninger), skal den behandlingsansvarlige anonymisere opplysningene for å sikre at de ikke lenger identifiserer en bestemt person, alene eller samkjørt med andre opplysninger, idet det tas rimelig hensyn til tid, kostnader, teknologi osv., i samsvar med artikkel 58-2 i PIPA.

5. **Korrigerende tiltak osv. (lovens artikkel 64 nr. 1, 2 og 4)**

<Loven om vern av personopplysninger

(lov nr. 16930, delvis endret 4. februar 2020)>

Artikkel 64 (korrigerende tiltak) 1. Dersom PIPC anser at det er vektige grunner til å anta at det har skjedd en overtredelse i forbindelse med personopplysninger, og at det dersom det ikke treffes tiltak, sannsynligvis vil forårsake skade som det er vanskelig å avhjelpe, kan den pålegge den som har overtrådt denne loven (unntatt sentrale forvaltningsorganer, lokale myndigheter, nasjonalforsamlingen, domstolen, forfatningsdomstolen og den nasjonale valgkommisjonen), å treffe følgende tiltak:

1. Stoppe overtredelsen i forbindelse med personopplysninger.
2. Midlertidig innstille behandlingen av personopplysninger.

([7]) På samme måte får unntaket i artikkel 40-3 i kredittopplysningsloven anvendelse på behandling av pseudonymiserte kredittopplysninger for statistiske formål og formål knyttet til vitenskapelig forskning og oppbevaring av offentlige registre.

3. Andre nødvendige tiltak for å verne personopplysninger og hindre overtredelser i forbindelse med personopplysninger.

2. Dersom lederen for et relatert sentralt forvaltningsorgan anser at det er vektige grunner til å anta at det har skjedd en overtredelse i forbindelse med personopplysninger, og at det dersom det ikke treffes tiltak, sannsynligvis vil forårsake skade som det er vanskelig å avhjelpe, kan vedkommende pålegge en behandlingsansvarlig å treffe noen av tiltakene nevnt i nr. 1 i henhold til lovgivningen i det relaterte sentrale forvaltningsorganets jurisdiksjon.

4. Dersom et sentralt forvaltningsorgan, en lokal myndighet, nasjonalforsamlingen, domstolen, forfatningsdomstolen eller den nasjonale valgkommisjonen bryter denne loven, kan PIPC anbefale lederen for det relevante organet å treffe noen av tiltakene nevnt i nr. 1. I slike tilfeller skal organet følge anbefalingen med det samme den mottas, med mindre det foreligger ekstraordinære omstendigheter.

i. For det første fortolker rettspraksis([8])([9]) «skade som det er vanskelig å avhjelpe» som noe som kan krenke en enkeltpersons personlige rettigheter eller personvern.

ii. Med «vektige grunner til å anta at det har skjedd en overtredelse i forbindelse med personopplysninger, og at det dersom det ikke treffes tiltak, sannsynligvis vil forårsake skade som det er vanskelig å avhjelpe» som nevnt i artikkel 64 nr. 1 og 2 menes tilfeller der en overtredelse av loven anses for å kunne krenke enkeltpersoners rettigheter og friheter i forbindelse med personopplysninger. Dette får anvendelse når noen av prinsippene, rettighetene og pliktene som inngår i loven for å verne personopplysninger, krenkes([10]).

iii. I henhold til artikkel 64 nr. 4 i loven om vern av personopplysninger er et tiltak i forbindelse med «overtredelse av denne loven» et tiltak mot en overtredelse av nevnte lov.

Et sentralt forvaltningsorgan osv. kan, i egenskap av å være en offentlig myndighet som er bundet av rettsstatsprinsippet, ikke bryte lover og plikter å treffe et korrigerende tiltak, herunder å stoppe handlingen umiddelbart, og gi skadeserstatning i de unntakstilfellene der det likevel er begått en ulovlig handling.

Et sentralt forvaltningsorgan osv. må dermed, også dersom PIPC ikke griper inn i henhold til artikkel 64 nr. 4 i PIPA, treffe et korrigerende tiltak mot overtredelser dersom det får kjennskap til en overtredelse av loven.

Dersom PIPC har anbefalt et korrigerende tiltak, vil det normalt, på en objektiv måte, være klart for det sentrale forvaltningsorganet osv. at det har overtrådt loven. For å begrunne hvorfor det mener at en anbefaling fra PIPC ikke bør følges, skal et sentralt forvaltningsorgan osv. framlegge klare grunner som kan bevise at det ikke har overtrådt loven. Anbefalingen skal følges, med mindre PIPC bestemmer at dette rent faktisk ikke er tilfellet.

På bakgrunn av dette skal de «ekstraordinære omstendighetene» i artikkel 64 nr. 4 i loven om vern av personopplysninger begrenses strengt til ekstraordinære omstendigheter der sentrale forvaltningsorganer osv. framlegger klare grunner som beviser at «denne loven faktisk ikke er overtrådt», for eksempel «tilfeller der det foreligger ekstraordinære (faktiske eller rettslige) omstendigheter» som PIPC ikke kjente til da den utarbeidet sin anbefaling, og PIPC fastslår at det rent faktisk ikke har skjedd en overtredelse.

6. **Anvendelse av loven om vern av personopplysninger på behandling av personopplysninger for formål knyttet til nasjonal sikkerhet, herunder etterforskning av overtredelser og håndheving i samsvar med nevnte lov (artikkel 7-8 og 7-9, artikkel 58, artikkel 3 og 4 og artikkel 62 i nevnte lov)**

<Loven om vern av personopplysninger

(lov nr. 16930, delvis endret 4. februar 2020)>

Artikkel 7-8 (PIPCs arbeid) 1. PIPC skal utføre følgende oppgaver: […]

3. Spørsmål som gjelder undersøkelse av krenking av registrertes rettigheter og disposisjonene som følger av dette.

4. Behandling av klager eller prosedyrer for avhjelpende tiltak i forbindelse med behandling av personopplysninger og mekling i tvister knyttet til personopplysninger.

[…]

([8]) (Høyesteretts dom 97Da10215,10222 av 26. januar 1999). Dersom informasjon om den tiltaltes straffbare handlinger avsløres via mediene, vil det sannsynligvis forårsake uopprettelig psykisk og fysisk skade ikke bare for offeret, det vil si saksøkeren, men også for personer rundt vedkommende, herunder familier.

([9]) (Seouls høyere domstols dom 2006Na92006 av 16. januar 2008). Dersom en ærekrenkende artikkel offentliggjøres, vil det sannsynligvis forårsake alvorlig uopprettelig skade for den berørte personen.

([10]) De sammen prinsippene som fastsatt i punkt ii) får anvendelse på artikkel 45-4 i kredittopplysningsloven.

Artikkel 7-9 (spørsmål som PIPC skal behandle og treffe beslutning om) 1. PIPC skal behandle og treffe beslutning om følgende spørsmål: […]

5. Spørsmål som gjelder fortolkning og anvendelse av lovgivningen knyttet til vern av personopplysninger.

[…]

Artikkel 58 (delvis unntak fra anvendelse) 1. Kapittel III–VII får ikke anvendelse på følgende personopplysninger:

1. Personopplysninger som samles inn i henhold til statistikkloven for å bli behandlet av offentlige institusjoner.
2. Personopplysninger som samles inn, eller som skal framlegges, med henblikk på analysering av informasjon knyttet til den nasjonale sikkerheten.
3. Personopplysninger som behandles midlertidig når det er tvingende nødvendig av hensyn til den offentlige sikkerheten, folkehelsen osv.
4. Personopplysninger som samles inn eller brukes av pressen for egne rapporteringsformål, religiøse organisasjoners misjonsvirksomhet og politiske partiers nominering av kandidater.

[Nr. 2 og 3 utelatt.]

4. I forbindelse med behandling av personopplysninger i henhold til nr. 1 skal en behandlingsansvarlig behandle personopplysninger i så lite omfang som nødvendig for å oppfylle det tiltenkte formålet, og i kortest mulig tid, og skal også treffe nødvendige tiltak, for eksempel tekniske, organisatoriske og fysiske garantier, sikre individuell klagebehandling og andre nødvendige tiltak for en sikker håndtering og egnet behandling av slike personopplysninger.

Artikkel 3 (prinsipper for vern av personopplysninger) 1. Den behandlingsansvarlige skal uttrykkelig angi formålene som personopplysninger behandles for, og skal samle inn personopplysninger på en lovlig og rettferdig måte i så lite omfang som nødvendig for å oppfylle disse formålene.

2. Den behandlingsansvarlige skal behandle personopplysninger på en måte som er egnet og nødvendig for formålene som personopplysningene behandles for, og skal ikke bruke dem for andre formål.

3. Den behandlingsansvarlige skal sikre at personopplysningene er riktige, fullstendige og oppdaterte i det omfanget som er nødvendig for formålene som personopplysningene behandles for.

4. Den behandlingsansvarlige skal håndtere personopplysninger på en sikker måte i henhold til behandlingsmetodene for og typene av osv. personopplysninger, idet det tas hensyn til risikoen for å krenke den registrertes rettigheter og hvor alvorlig den relevante risikoen er.

5. Den behandlingsansvarlige skal offentliggjøre sitt personvernprogram og andre elementer knyttet til behandlingen av personopplysninger og skal garantere den registrertes rettigheter, for eksempel retten til innsyn i egne personopplysninger.

6. Den behandlingsansvarlige skal behandle personopplysninger på en måte som minimerer muligheten for å krenke en registrerts personvern.

7. Dersom det fortsatt er mulig å oppfylle formålet med innsamlingen av personopplysninger ved å behandle anonymiserte eller pseudonymiserte personopplysninger, skal den behandlingsansvarlige bestrebe seg på å behandle personopplysninger gjennom anonymisering dersom anonymisering er mulig, eller gjennom pseudonymisering dersom det ikke er mulig å oppfylle formålet med innsamlingen av personopplysninger gjennom anonymisering.

8. Den behandlingsansvarlige skal bestrebe seg på å vinne de registrertes tillit ved å overholde og utføre oppgavene og ansvaret fastsatt i denne loven og i andre relaterte lover.

Artikkel 4 (registrertes rettigheter) En registrert har følgende rettigheter i forbindelse med behandlingen av vedkommendes personopplysninger:

1. Retten til å bli informert om behandlingen av slike personopplysninger.
2. Retten til å avgjøre om det skal gis samtykke til behandlingen av personopplysninger, og omfanget av samtykket.
3. Retten til å få bekreftet om personopplysninger behandles, og til å be om innsyn (herunder utlevering av kopier, heretter gjelder det samme) i slike personopplysninger.
4. Retten til å få innstilt behandlingen av slike personopplysninger og til å be om at de rettes, slettes og tilintetgjøres.
5. Retten til egnet erstatning for skader som oppstår som følge av behandlingen av slike personopplysninger, ved hjelp av en rask og rettferdig prosedyre.

Artikkel 62 (rapportering av overtredelser) 1. Enhver som har fått sine rettigheter eller interesser krenket i forbindelse med en behandlingsansvarligs behandling av vedkommendes personopplysninger, kan rapportere dette til PIPC.
2. PIPC kan utpekte en spesialisert institusjon som skal motta og behandle disse klagene i henhold til nr. 1, som fastsatt ved presidentdekret. I slike tilfeller skal en slik spesialisert institusjon opprette og drive en telefontjeneste for overtredelser i forbindelse med personopplysninger (heretter kalt «personverntelefontjeneste»).
3. Personverntelefontjenesten skal utføre følgende oppgaver:
1. Motta rapporter og gi rådgivning i forbindelse med behandling av personopplysninger.

2. Undersøke og bekrefte hendelser og innhente uttalelser fra berørte parter.

3. Oppgaver i tilknytning til nr. 1 og 2.

4. PIPC kan ved behov sende en offentlig tjenestemann til den spesialiserte institusjonen som er utpekt i henhold til nr. 2 i samsvar med artikkel 32-4 i loven om offentlig ansatte, for å undersøke og bekrefte hendelsene i henhold til nr. 3 pkt. 2.

i) Innsamlingen av personopplysninger for formål knyttet til nasjonal sikkerhet reguleres av særlige lover som gir vedkommende myndigheter (for eksempel den nasjonale etterretningstjenesten) myndighet til å avlytte kommunikasjon eller anmode om utlevering på visse vilkår og med visse garantier (heretter kalt «nasjonal sikkerhetslovgivning»). Denne nasjonale sikkerhetslovgivningen omfatter for eksempel loven om personvern i forbindelse med kommunikasjon, loven om terrorbekjempelse og beskyttelse av borgere og den offentlige sikkerhet eller loven om telekommunikasjonsvirksomhet. Innsamlingen og den videre behandlingen av personopplysninger skal dessuten oppfylle kravene i PIPA. I denne forbindelse er det i artikkel 58 nr. 1 pkt. 2 i PIPA fastsatt at kapittel III–VII ikke får anvendelse på personopplysninger som samles inn, eller som skal framlegges, med henblikk på analysering av informasjon knyttet til nasjonal sikkerhet. Dette delvise unntaket får derfor anvendelse på behandling av personopplysninger for formål knyttet til nasjonal sikkerhet.

   Samtidig får kapittel I (generelle bestemmelser), kapittel II (fastsettelse av strategier for vern av personopplysninger osv.), kapittel VIII (kollektive søksmål ved overtredelser knyttet til personopplysninger), kapittel IX (tilleggsbestemmelser) og kapittel X (bestemmelser om sanksjoner) i PIPA anvendelse på behandling av slike personopplysninger. Dette omfatter de generelle prinsippene for vern av personopplysninger fastsatt i artikkel 3 (prinsipper for vern av personopplysninger) og de individuelle rettighetene som sikres ved artikkel 4 i PIPA (registrertes rettigheter).

   I artikkel 58 nr. 4 i PIPA er det dessuten fastsatt at slike opplysninger skal behandles i så lite omfang som nødvendig for å oppfylle det tiltenkte formålet, og i kortest mulig tid, i tillegg til at den behandlingsansvarlige skal treffe nødvendige tiltak for å sikre en sikker håndtering av opplysningene og egnet behandling, for eksempel tekniske, organisatoriske og fysiske garantier, og tiltak for egnet behandling av individuelle klager.

   Bestemmelsene om PIPCs oppgaver og myndighet (herunder artikkel 60–65 i PIPA om behandling av klager og vedtakelse av anbefalinger og korrigerende tiltak) samt bestemmelsene om administrative og strafferettslige sanksjoner (artikkel 70 ff. i PIPA) får anvendelse. I henhold til artikkel 7-8 nr. 1 pkt. 3 og 4 og artikkel 7-9 nr. 1 pkt. 5 i PIPA omfatter denne undersøkelsesmyndigheten og myndigheten til å treffe korrigerende tiltak, herunder når den utøves i forbindelse med behandling av klager, også mulige overtredelser av reglene i spesifikke lover der det er fastsatt begrensninger og garantier med hensyn til innsamling av personopplysninger, herunder den nasjonale sikkerhetslovgivningen. Med hensyn til kravene i artikkel 3 nr. 1 i PIPA om lovlig og rettferdig innsamling av personopplysninger utgjør en slik overtredelse en overtredelse av «denne loven» i henhold til artikkel 63 og 64, noe som gjør det mulig for PIPC å foreta en undersøkelse og treffe korrigerende tiltak([11]). PIPCs utøvelse av slik myndighet utfyller, men erstatter ikke den nasjonale menneskerettighetskommisjonens myndighet i henhold til loven om menneskerettighetskommisjonen.

   Anvendelsen av de grunnleggende prinsippene, rettighetene og pliktene i PIPA på behandlingen av personopplysninger for formål knyttet til nasjonal sikkerhet gjenspeiler garantiene som er nedfelt i forfatningen for å verne av enkeltpersoners rett til å kontrollere sine egne personopplysninger. Som anerkjent av forfatningsdomstolen omfatter dette en persons rett([12]) «til selv å bestemme når, til hvem og av hvem og i hvilket omfang vedkommendes personopplysninger skal utleveres eller brukes. Det er en grunnleggende rettighet([13]) […] som skal verne den enkeltes beslutningsfrihet mot risikoen som utvidelsen av statlige funksjoner og informasjons- og kommunikasjonsteknologi medfører». Enhver begrensning av denne rettigheten, for eksempel når det er nødvendig for å beskytte den nasjonale sikkerheten, krever at den enkeltes rettigheter og interesser avveies mot den relevante allmenne interessen, og må ikke berøre rettighetens vesentlige innhold (artikkel 37 nr. 2 i forfatningen).

([11]) Når det gjelder korrigerende tiltak i henhold til artikkel 64, se også avsnitt 5 over.
([12]) Forfatningsdomstolens dom 99HunMa513, 2004HunMa190 av 26. mai 2005.
([13]) Forfatningsdomstolens dom 2003HunMa282 av 21. juli 2005.

Ved behandling av personopplysninger for formål knyttet til nasjonal sikkerhet skal den behandlingsansvarlige (det vil si NIS) derfor blant annet gjøre følgende:

1. Uttrykkelig angi formålene som personopplysningene behandles for, og samle inn personopplysninger på en lovlig og rettferdig måte og i så lite omfang som nødvendig for å oppfylle formålene (artikkel 3 nr. 1 i PIPA). Den behandlingsansvarlige skal bare samle inn og viderebehandle personopplysningene for å utføre oppgaver i henhold til relevant lovgivning, for eksempel loven om den nasjonale etterretningstjenesten.

2. Behandle personopplysninger i så lite omfang som og ikke lenger enn nødvendig for å oppfylle det tiltenkte formålet (artikkel 58 nr. 4 i PIPA). Når formålet med behandlingen er oppnådd, skal den behandlingsansvarlige tilintetgjøre personopplysningene på en måte som gjør at de ikke kan gjenopprettes, med mindre videre lagring er uttrykkelig fastsatt ved lov, da skal de relevante personopplysningene lagres og forvaltes atskilt fra andre personopplysninger, ikke brukes for andre formål enn formålet angitt i loven og tilintetgjøres når lagringsperioden er utløpt.

3. Behandle personopplysninger på en måte som er egnet og nødvendig for formålene som personopplysningene behandles for, og ikke bruke dem for andre formål (artikkel 3 nr. 2 i PIPA).

4. Sikre at personopplysninger er riktige, fullstendige og oppdaterte i det omfanget som er nødvendig for formålene som personopplysningene behandles for (artikkel 3 nr. 3 i PIPA).

5. Håndtere personopplysninger på en sikker måte i henhold til behandlingsmetodene for og typene av osv. personopplysninger, idet det tas hensyn til risikoen for å krenke den registrertes rettigheter og hvor alvorlig den aktuelle risikoen er (artikkel 3 nr. 4 i PIPA).

6. Offentliggjøre sitt personvernprogram og andre elementer som er knyttet til behandling av personopplysninger (artikkel 3 nr. 5 i PIPA).

7. Behandle personopplysninger på en måte som minimerer risikoen for å krenke den registrertes personvern (artikkel 3 nr. 6 i PIPA).

ii) I samsvar med artikkel 58 nr. 4 i PIPA skal den behandlingsansvarlige (for eksempel myndigheter med ansvar for nasjonal sikkerhet, for eksempel NIS) treffe nødvendige tiltak, for eksempel innføre tekniske, organisatoriske og fysiske garantier for å sikre overholdelse av disse prinsippene og egnet behandling av personopplysninger. Dette kan for eksempel omfatte særlige tiltak for å garantere personopplysningenes sikkerhet, for eksempel begrensninger i tilgangen til personopplysninger, tilgangskontroller, logger, målrettet opplæring av ansatte i håndtering av personopplysninger osv.

I samsvar med artikkel 3 nr. 5 og 4 i PIPA har de registrerte dessuten blant annet følgende rettigheter med hensyn til personopplysninger som behandles for formål knyttet til nasjonal sikkerhet:

1. Retten til å få en bekreftelse på om vedkommendes personopplysninger behandles, og opplysninger om behandlingen og tilgang til disse opplysningene, herunder til å få utlevert kopier (artikkel 4 nr. 1 og 3 i PIPA).

2. Retten til å få behandlingen innstilt og til å få rettet, slettet og tilintetgjort personopplysninger (artikkel 4 nr. 4 i PIPA).

iii) I forbindelse med utøvelsen av disse rettighetene kan den registrerte inngi en anmodning direkte til den behandlingsansvarlige eller indirekte via PIPC samt kan gi sin representant tillatelse til å gjøre dette. Dersom den registrerte inngir en anmodning, skal den behandlingsansvarlige gi rettigheten uten opphold. Den behandlingsansvarlige kan imidlertid utsette, begrense eller nekte å gi rettigheten dersom det er uttrykkelig fastsatt eller uunngåelig for å overholde andre lover, i den grad og så lenge det er nødvendig og forholdsmessig for å beskytte et viktig mål av allmenn interesse (for eksempel i den grad og så lenge det å gi rettigheten vil bringe en pågående etterforskning i fare eller true den nasjonale sikkerheten), eller dersom det å gi rettigheten kan skade en tredjeparts liv eller legeme eller urettmessig krenke en tredjeparts eiendom og andre interesser. Dersom anmodningen avslås eller begrenses, skal den behandlingsansvarlige uten opphold underrette den registrerte. Den behandlingsansvarlige skal utarbeide en metode og en framgangsmåte som gjør det mulig for registrerte å inngi anmodninger, og offentliggjøre dem, slik at de registrerte får kjennskap til dem.

I samsvar med artikkel 58 nr. 4 i PIPA (krav om å sikre egnet behandling av individuelle klager) og artikkel 4 nr. 5 i PIPA (retten til egnet erstatning for enhver skade som følger av behandlingen av personopplysninger, gjennom en rask og rettferdig prosedyre), har registrerte dessuten rett til prøving. Dette omfatter retten til å rapportere en påstått overtredelse til senteret for rapportering av overtredelser i forbindelse med personopplysninger (i samsvar med artikkel 62 nr. 3 i PIPA), inngi en klage til PIPC i henhold til artikkel 62 i PIPA om enhver krenking av rettigheter eller interesser knyttet til en persons personopplysninger og å oppnå rettslig prøving av PIPCs beslutninger eller unnlatelse av å handle i henhold til forvaltningsprosessloven. De registrerte har dessuten rett til rettslig prøving i henhold til forvaltningsprosessloven dersom deres rettigheter eller interesser er blitt krenket som følge av en disposisjon eller unnlatelse fra den behandlingsansvarliges side (for eksempel ulovlig innsamling av personopplysninger), eller til skadeserstatning i samsvar med loven om statlig erstatning. Disse rettsmidlene er tilgjengelige både ved mulige overtredelser av reglene i spesifikke lover der det er fastsatt særlige begrensninger og garantier for innsamling av personopplysninger, for eksempel den nasjonale sikkerhetslovgivningen, og i PIPA.

En EU-borger kan klage til PIPC via vedkommendes nasjonale personvernmyndighet, og PIPC vil underrette vedkommende via den nasjonale personvernmyndigheten når undersøkelsen og det korrigerende tiltaket (dersom det er relevant) er avsluttet.

———

VEDLEGG II

18. mai 2021

Didier Reynders, kommissær for justis i Europakommisjonen

Deres eksellense

Jeg gleder meg over de konstruktive drøftingene mellom Republikken Korea og Europakommisjonen med det formålet å skape en ramme for overføring av personopplysninger fra EU til Republikken Korea.

På Europakommisjonens anmodning til den sørkoreanske regjeringen sender jeg vedlagte dokument, som gir en oversikt over den rettslige rammen for sørkoreanske myndigheters tilgang til opplysninger.

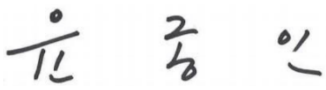
Dette dokumentet gjelder en rekke departementer og organer i Republikken Korea, og når det gjelder dokumentets innhold er de relevante departementene og organene (kommisjonen for vern av personopplysninger, justisdepartementet, den nasjonale etterretningstjenesten, Republikken Koreas nasjonale menneskerettighetskommisjon, det nasjonale senteret for terrorbekjempelse, Republikken Koreas enhet for finansiell etterretning) ansvarlige for de delene som omfatter deres respektive kompetanseområder. De relevante departementene og organene er angitt nedenfor sammen med deres respektive underskrifter.

Kommisjonen for vern av personopplysninger vil motta alle forespørsler vedrørende dette dokumentet og vil samordne de nødvendige svarene fra de vedkommende departementene og organene.

Jeg håper at dette dokumentet vil være til hjelp for Europakommisjonens beslutningstaking.

Jeg setter stor pris på Deres store bidrag i denne saken så langt.

Med vennlig hilsen



Yoon Jong In
Formann for kommisjonen for vern av personopplysninger

Dette dokumentet er utarbeidet av kommisjonen for vern av personopplysninger og følgende berørte departementer og organer:

Park Jie Won
President (direktør), den nasjonale etterretningstjenesten

Lee Jung Soo
Generaldirektør, justisdepartementet

Choi Young Ae
Formann, Republikken Koreas nasjonale menneskerettighetskommisjon

Kim Hyuck Soo
Direktør, det nasjonale senteret for terrorbekjempelse

Kim, Jeong Kag
Kommissær, Republikken Koreas enhet for finansiell etterretning

Rettslig ramme for sørkoreanske offentlige myndigheters innsamling og bruk av personopplysninger for formål knyttet til rettshåndheving og nasjonal sikkerhet

Følgende dokument gir en oversikt over den rettslige rammen for sørkoreanske offentlige myndigheters innsamling og bruk av personopplysninger for formål knyttet til strafferettslig håndheving og nasjonal sikkerhet (heretter kalt «offentlige myndigheters tilgang»), særlig når det gjelder tilgjengelig rettslig grunnlag, gjeldende vilkår (begrensninger) og garantier samt uavhengig tilsyn og muligheter for individuell prøvings- og klageadgang.

1. GENERELLE RETTSPRINSIPPER SOM ER RELEVANTE FOR OFFENTLIGE MYNDIGHETERS TILGANG

1.1. Forfatningsmessig ramme

I Republikken Koreas forfatning er retten til personvern generelt (artikkel 17) og retten til personvern i forbindelse med korrespondanse spesielt (artikkel 18) fastsatt. Det er statens plikt å garantere disse grunnleggende rettighetene([1]). I forfatningen er det videre fastsatt at borgernes rettigheter og friheter bare kan begrenses ved lov når det er nødvendig av hensyn til den nasjonale sikkerheten eller for å opprettholde lov og orden med henblikk på borgernes velferd([2]). Selv når det innføres slike begrensninger, kan de ikke berøre frihetens eller rettighetens vesentlige innhold([3]). De sørkoreanske domstolene har anvendt disse bestemmelsene i saker som har hatt med statlig inngripen i personvernet å gjøre. Høyesterett har for eksempel fastslått at overvåking av sivile krenker den grunnleggende retten til personvern, og har understreket at borgerne har «rett til selvbestemmelse over personopplysninger»([4]). I et annet tilfelle har forfatningsdomstolen fastslått at personvern er en grunnleggende rettigheter som gir beskyttelse mot statlig inngripen i og overvåking av borgernes privatliv([5]).

Ved den sørkoreanske forfatningen garanteres det videre at ingen skal arresteres, holdes i varetekt, ransakes, avhøres eller få gjenstander beslaglagt, unntatt i de tilfellene som er fastsatt ved lov([6]). Videre kan ransaking og beslaglegging bare foretas på grunnlag av en rettskjennelse utstedt på anmodning fra en påtalemyndighet og ved overholdelse av prinsippet om rettferdig rettergang([7]). Under ekstraordinære omstendigheter, det vil si dersom en mistenkt pågripes på fersk gjerning (*in flagranti*), eller dersom det er fare for at en person som er mistenkt for å ha begått en straffbar handling som kan straffes med fengsel i minst tre, kan unnslippe eller ødelegge bevismateriale, kan etterforskningsmyndighetene foreta ransaking eller beslaglegging uten kjennelse, og skal da framsette en begjæring om kjennelse i ettertid([8]). Disse generelle prinsippene utvikles videre i spesifikke lover om straffeprosesser og vern av kommunikasjon (se den detaljerte oversikten nedenfor).

Når det gjelder fremmede borgere, er det i forfatningen fastsatt at deres status garanteres i henhold til folkeretten og internasjonale traktater([9]). En rekke internasjonale avtaler som Republikken Korea er part i, garanterer retten til personvern, for eksempel den internasjonale konvensjonen om sivile og politiske rettigheter (artikkel 17), konvensjonen om rettighetene til mennesker med nedsatt funksjonsevne (artikkel 22) og konvensjonen om barns rettigheter (artikkel 16). Selv om det i forfatningen i prinsippet vises til «statsborgeres» rettigheter, har forfatningsdomstolen fastslått at fremmede borgere også har grunnleggende rettigheter([10]). Domstolen har særlig fastslått at vern av en persons verdighet og verdi som menneske samt retten

([1]) Artikkel 10 i Republikken Koreas forfatning som ble offentliggjort 17. juli 1948 (heretter kalt «forfatningen»).
([2]) Artikkel 37 nr. 2 i forfatningen.
([3]) Artikkel 37 nr. 2 i forfatningen.
([4]) Republikken Koreas høyesteretts avgjørelse 96DA42789 av 24. juli 1998.
([5]) Forfatningsdomstolens avgjørelse 2002Hun-Ma51 av 30. oktober 2003. På samme måte presiserte forfatningsdomstolen i avgjørelse 99Hun-Ma513 og 2004Hun-Ma190 (konsolidert) av. 26. mai 2005 at «retten til å kontrollere egne personopplysninger er en rett som den personen som opplysningene gjelder, har til å bestemme når, til hvem eller av hvem og i hvilket omfang vedkommendes opplysninger skal utleveres eller brukes. Det er en grunnleggende rettighet, selv om den ikke er spesifisert i forfatningen, som skal beskytte den enkeltes beslutningsfrihet mot risikoen som utvidelsen av statlige funksjoner og informasjons- og kommunikasjonsteknologi medfører».
([6]) Artikkel 12 nr. 1 første punktum i forfatningen.
([7]) Artikkel 16 og 12 nr. 3 i forfatningen.
([8]) Artikkel 12 nr. 3 i forfatningen.
([9]) Artikkel 6 nr. 2 i forfatningen.
([10]) Forfatningsdomstolens avgjørelse 93Hun-MA120 av 29. desember 1994. Se også for eksempel forfatningsdomstolens avgjørelse 2014Hun-Ma346 av 31. mai 2018 der domstolen konstaterte at den forfatningsmessige retten til en sudansk statsborger som var holdt tilbake i lufthavnen, til juridisk bistand var blitt krenket. I en annen sak konstaterte forfatningsdomstolen at friheten til å velge sin egen lovlige arbeidsplass er nært knyttet til retten til å strebe etter lykke samt menneskers verdighet og verdi, og at den derfor ikke bare er forbeholdt statsborgere, men også kan garanteres utlendinger som er lovlig ansatt i Republikken Korea (forfatningsdomstolens avgjørelse 2007Hun-Ma1083 av 29. september 2011).

til å strebe etter lykke er rettigheter som ethvert menneske har, og ikke bare statsborgere([11]). Domstolen har også presisert at retten til å bestemme over egne opplysninger anses som en grunnleggende rettighet som bygger på retten til verdighet og streben etter lykke og retten til personvern([12]). Selv om rettspraksisen fram til i dag ikke spesifikt har behandlet ikke-sørkoreanske borgeres rett til personvern, er det allment akseptert blant spesialister at «menneskers rettigheter» er fastsatt i forfatningens artikkel 12-22 (som omfatter retten til personvern og personlig frihet).

Forfatningen sikrer også retten til å kreve en rimelig erstatning fra offentlige myndigheter([13]). På grunnlag av loven om forfatningsdomstolen kan enhver person som får sine grunnleggende forfatningssikrede rettigheter krenket gjennom utøvelse av offentlig myndighet (unntatt domstolsavgjørelser), dessuten inngi en forfatningsmessig klage til forfatningsdomstolen([14]).

1.2. **Generelle regler for vern av opplysninger**

Den generelle loven for vern av opplysninger i Republikken Korea, loven om vern av personopplysninger (Personal Information Protection Act, heretter kalt «PIPA»), får anvendelse på både privat og offentlig sektor. Når det gjelder offentlige myndigheter, vises det i PIPA spesifikt til plikten til å utarbeide strategier for å hindre «misbruk og feil bruk av person-opplysninger, gjennomgripende overvåking og sporing osv. og for å styrke menneskers verdighet og personvern»([15]).

Behandling av personopplysninger for rettshåndhevende formål er underlagt alle kravene i PIPA. Dette betyr for eksempel at strafferettshåndhevende myndigheter skal overholde forpliktelsene som gjelder behandlingens lovlighet, det vil si at innsamlingen, bruken eller videreformidlingen av personopplysninger skal være basert på en av de rettslige grunnene angitt i PIPA (artikkel 15–18 i PIPA) og være i samsvar med prinsippene om formålsbegrensning (artikkel 3 nr. 1 og 2 i PIPA), forholdsmessighet/dataminimering (artikkel 3 nr. 1 og 6 i PIPA), begrenset lagring av opplysningene (artikkel 21 i PIPA), opplysningssikkerhet, herunder underretning om brudd på opplysningssikkerheten (artikkel 3 nr. 4 og artikkel 29 og 34 i PIPA) og åpenhet (artikkel 3 nr. 1 og 5 og artikkel 20, 30 og 32 i PIPA). For sensitive opplysninger gjelder det spesifikke garantier (artikkel 23 i PIPA). I samsvar med artikkel 3 nr. 5, artikkel 4 og artikkel 35–39-2 i PIPA kan enkeltpersoner dessuten utøve sin rett til innsyn, retting, sletting og innstilling av behandlingen overfor rettshåndhevende myndigheter.

PIPA får derfor fullt ut anvendelse på behandling av personopplysninger for formål knyttet til strafferettslig håndheving, men inneholder et unntak når personopplysninger behandles for formål knyttet til nasjonal sikkerhet. I henhold til artikkel 58 nr. 1 pkt. 2 i PIPA får artikkel 15–50 i PIPA ikke anvendelse på personopplysninger som samles inn eller som det anmodes om med henblikk på analysering av informasjon knyttet til nasjonal sikkerhet([16]). Kapittel I (generelle bestemmelser), kapittel II (fastsettelse av strategier for vern av personopplysninger osv.), kapittel VIII (kollektive søksmål ved overtredelser knyttet til personopplysninger), kapittel IX (tilleggsbestemmelser) og kapittel X (bestemmelser om sanksjoner) i PIPA gjelder derimot. Dette omfatter de generelle prinsippene for vern av personopplysninger fastsatt i artikkel 3 (prinsipper for vern av person-opplysninger) og de individuelle rettighetene som sikres ved artikkel 4 i PIPA (registrertes rettigheter). Dette betyr at de viktigste prinsippene og rettighetene er garantert også på dette området. I artikkel 58 nr. 4 i PIPA er det dessuten fastsatt at slike opplysninger skal behandles i så lite omfang som nødvendig for å oppfylle det tiltenkte formålet, og i kortest mulig tid, og at den behandlingsansvarlige skal treffe nødvendige tiltak for å sikre en sikker håndtering av opplysningene og egnet behandling, for eksempel tekniske, organisatoriske og fysiske garantier, og tiltak for å sikre egnet behandling av individuelle klager.

I melding 2021-1 om utfyllende regler for fortolkning og anvendelse av loven om vern av personopplysninger har kommisjonen for vern av personopplysninger (Personal Information Protection Commission, heretter kalt «PIPC») ytterligere presisert hvordan PIPA får anvendelse på behandling av personopplysninger for formål knyttet til nasjonal sikkerhet i lys av dette delvise unntaket([17]). Dette omfatter særlig enkeltpersoners rettigheter (innsyn, retting, sletting og innstilling av behandlingen) og begrunnelsene for disse rettighetene og grenser for eventuelle begrensninger av dem. I henhold til meldingen gjenspeiler anvendelsen av de grunnleggende prinsippene, rettighetene og pliktene i PIPA på behandlingen av personopplysninger for

([11]) Forfatningsdomstolens avgjørelse 99HeonMa494 av 29. november 2001.
([12]) Se for eksempel forfatningsdomstolens avgjørelse 99HunMa513.
([13]) Artikkel 29 nr. 1 i forfatningen.
([14]) Artikkel 68 nr. 1 i loven om forfatningsdomstolen.
([15]) Artikkel 5 nr. 1 i PIPA.
([16]) Artikkel 58 nr. 1 pkt. 2 i PIPA.
([17]) Melding 2021-1 fra PIPC om utfyllende regler for fortolkning og anvendelse av loven om vern av personopplysninger, avsnitt III nr. 6.

formål knyttet til nasjonal sikkerhet garantiene som er fastsatt i forfatningen for å verne enkeltpersoners rett til å kontrollere sine egne personopplysninger. Enhver begrensning av denne rettigheten, for eksempel når det er nødvendig for å beskytte den nasjonale sikkerheten, krever at den enkeltes rettigheter og interesser avveies mot den relevante allmenne interessen, og må ikke berøre rettighetens vesentlige innhold (artikkel 37 nr. 2 i forfatningen).

2. OFFENTLIGE MYNDIGHETERS TILGANG FOR RETTSHÅNDHEVENDE FORMÅL

2.1. Vedkommende offentlige myndigheter på området rettshåndheving

På grunnlag av straffeprosessloven (Criminal Procedure Act, heretter kalt «CPA»), loven om personvern i forbindelse med kommunikasjon (Communications Privacy Protection Act, heretter kalt «CPPA») og loven om telekommunikasjonsvirksomhet (Telecommunications Business Act, heretter kalt «TBA») kan politiet, påtalemyndigheter og domstoler samle inn personopplysninger for formål knyttet til strafferettslig håndheving. I den grad loven om den nasjonale etterretningstjenesten gir denne myndigheten også til den nasjonale etterretningstjenesten (National Intelligence Service, heretter kalt «NIS») skal den overholde de ovennevnte lovene([18]). Loven om rapportering og bruk av spesifikke opplysninger om finansielle transaksjoner (Act on Reporting and Using Specified Financial Transaction Information, heretter kalt «ARUSFTI») utgjør et rettslig grunnlag for at finansielle institusjoner kan utlevere opplysninger til Republikken Koreas enhet for finansiell etterretning (Korea Financial Intelligence Unit, heretter kalt «KOFIU») med henblikk på å forebygge hvitvasking av penger og finansiering av terrorisme. Denne spesialiserte enheten kan videreformidle slike opplysninger til rettshåndhevende myndigheter. Denne utleveringsplikten får imidlertid bare anvendelse på behandlingsansvarlige som behandler personlige kredittopplysninger i henhold til kredittopplysningsloven, og som er underlagt kommisjonen for finansielle tjenesters tilsyn. Ettersom slike behandlingsansvarliges behandling av personlige kredittopplysninger ikke omfattes av virkeområdet for beslutningen om tilstrekkelige beskyttelsesnivå, er begrensningene og garantiene som gjelder i henhold til ARUSFTI, ikke beskrevet nærmere i dette dokumentet.

2.2. Rettslig grunnlag og begrensninger

CPA (se avsnitt 2.2.1), CPPA (se avsnitt 2.2.2) og loven om telekommunikasjonsvirksomhet (se avsnitt 2.2.3) danner det rettslige grunnlaget for innsamling av personopplysninger for rettshåndhevende formål og fastsetter gjeldende begrensninger og garantier.

2.2.1. *Ransaking og beslaglegging*

2.2.1.1. Rettslig grunnlag

Representanter for påtalemyndigheten og høyere tjenestemenn i kriminalpolitiet kan bare inspisere gjenstander, ransake personer eller beslaglegge gjenstander 1) dersom en person mistenkes for å ha begått en straffbar handling (en mistenkt), 2) dersom det er nødvendig for etterforskningen, og 3) dersom gjenstandene som skal inspiseres, personene som skal ransakes, og eventuelle gjenstander som beslaglegges, anses for å ha tilknytning til saken([19]). Domstolene kan også foreta ransaking og beslaglegge gjenstander som skal brukes som bevismateriale, eller som kan konfiskeres, så lenge slike gjenstander eller personer anses for å ha tilknytning til en bestemt sak([20]).

2.2.1.2. Begrensninger og garantier

Som en generell forpliktelse skal påtalemyndigheter og kriminalpolitiet respektere den mistenktes og enhver annen berørt persons menneskerettigheter([21]). Det kan i tillegg bare treffes tvangstiltak for å oppnå formålet med etterforskningen dersom det er uttrykkelig fastsatt i CPA, og bare i den grad det er strengt nødvendig([22]).

Politiets eller påtalemyndigheters ransakinger, inspeksjoner eller beslaglegging som et ledd i en strafferettslig etterforskning må bare finne sted på grunnlag av en rettskjennelse([23]). Myndigheten som framsetter en begjæring om kjennelse, skal framlegge dokumentasjon som angir grunnen til at en person mistenkes for å ha begått en straffbar handling, at ransakingen, inspeksjonen eller beslagleggingen er nødvendig, og at de relevante gjenstandene som skal beslaglegges, finnes([24]). Kjennelsen skal blant annet inneholde navnet på den mistenkte og en beskrivelse av den straffbare handlingen, stedet, personen eller gjenstandene som skal ransakes, eller gjenstandene som skal beslaglegges, utstedelsesdatoen og den faktiske anvendelsesperioden([25]). Når det foretas ransaking og beslaglegging som et ledd i verserende rettssaker på annen måten enn i et offentlig rettsmøte, skal det også innhentes en rettskjennelse på forhånd([26]). Den berørte personen og vedkommendes forsvarer skal underrettes på forhånd om ransakingen eller beslagleggingen og kan være til stede når kjennelsen iverksettes([27]).

([18]) Se artikkel 3 i NIS-loven (lov nr. 12948) som gjelder strafferettslig etterforskning av visse straffbare handlinger, for eksempel opprør, oppstand og straffbare handlinger knyttet til nasjonal sikkerhet (for eksempel spionasje). Prosedyrene i CPA som gjelder ransaking og beslaglegging, får anvendelse i en slik sammenheng, mens CPPA regulerer innsamlingen av kommunikasjonsopplysninger (se del 3 om bestemmelsene om tilgang til kommunikasjon for formål knyttet til nasjonal sikkerhet).
([19]) Artikkel 215 nr. 1 og 2 i CPA.
([20]) Artikkel 106 nr. 1 og artikkel 107 og 109 i CPA.
([21]) Artikkel 198 nr. 2 i CPA.
([22]) Artikkel 199 nr. 1 i CPA.
([23]) Artikkel 215 nr. 1 og 2 i CPA.
([24]) Artikkel 108 nr. 1 i straffeprosessforordningen.
([25]) Artikkel 114 nr. 1 i CPA sammenholdt med artikkel 219 i CPA.
([26]) Artikkel 113 i CPA.
([27]) Artikkel 121 og 122 i CPA.

Når det foretas ransaking eller beslaglegging der gjenstanden som skal ransakes, er en disk på en datamaskin eller et annet datalagringsmedium, er det i prinsippet bare opplysningene (kopiert eller skrevet ut) som vil bli beslaglagt, og ikke hele mediet([28]). Datalagringsmediet kan bare beslaglegges dersom det anses som praktisk umulig å skrive ut eller kopiere de aktuelle opplysningene separat eller oppfylle formålet med ransakingen på annen måte([29]). Den berørte personen skal uten opphold underrettes om beslagleggingen([30]). CPA inneholder ingen unntak fra dette kravet om underretning.

Ransaking, undersøkelse og beslaglegging uten kjennelse kan bare foretas i begrensede situasjoner. For det første når det er umulig å innhente en kjennelse fordi situasjonen på gjerningsstedet gjør at det ikke er tid til det([31]). Det skal imidlertid uten opphold innhentes en kjennelse i ettertid([32]). For det andre kan det foretas ransaking og undersøkelse på stedet uten kjennelse når en mistenkt pågripes eller holdes i varetekt([33]). For det tredje kan påtalemyndigheten eller en høyere tjenestemann ved kriminalpolitiet beslaglegge en gjenstand uten kjennelse dersom gjenstanden er blitt kastet av en mistenkt eller en tredjeperson eller er blitt frivillig utlevert([34]).

Bevismateriale som er framskaffet i strid med CPA, godtas ikke([35]). I henhold til straffeloven straffes ulovlig ransaking av personer eller en persons bosted, bevoktede bygninger, strukturer, biler, skip, luftfartøyer eller bebodde lokaler dessuten med fengsel i opptil tre år([36]). Denne bestemmelsen får derfor også anvendelse når gjenstander, for eksempel datalagringsutstyr, beslaglegges under en ulovlig ransaking.

2.2.2. *Innsamling av kommunikasjonsopplysninger*

2.2.2.1. Rettslig grunnlag

Innsamlingen av kommunikasjonsopplysninger reguleres av en spesifikk lov – CPPA. Ved CPPA forbys særlig enhver sensur av post, avlytting av telekommunikasjon, videreformidling av kommunikasjonsbekreftelsesdata eller registrering av eller lytting til samtaler mellom personer som ikke er offentliggjort, unntatt på grunnlag av CPA, CPPA eller loven om militærdomstolen([37]). Begrepet «kommunikasjon» i betydningen angitt i CPPA omfatter både vanlig post og telekommunikasjon([38]). I denne forbindelse skiller CPPA mellom «kommunikasjonsbegrensende tiltak»([39]) og innsamling av «kommunikasjonsbekreftelsesdata».

Begrepet kommunikasjonsbegrensende tiltak omfatter «sensur», det vil si innsamling av innholdet i tradisjonell post, og «avlytting», det vil si direkte avlytting (innsamling eller opptak) av innholdet i telekommunikasjon([40]). Begrepet kommunikasjonsbekreftelsesdata omfatter «data om telekommunikasjonsregistreringer», herunder datoen og start- og sluttidspunktet for telekommunikasjoner, antall utgående og innkommende samtaler samt den andre partens abonnentnummer, bruksfrekvens, loggfiler om bruken av telekommunikasjonstjenester og lokaliseringsopplysninger (for eksempel fra signalmaster der signaler mottas)([41]).

([28]) Artikkel 106 nr. 3 i CPA.
([29]) Artikkel 106 nr. 3 i CPA.
([30]) Artikkel 219 sammenholdt med artikkel 106 nr. 4 i CPA.
([31]) Artikkel 216 nr. 3 i CPA.
([32]) Artikkel 216 nr. 3 i CPA.
([33]) Artikkel 216 nr. 1 og 2 i CPA.
([34]) Artikkel 218 i CPA. Når det gjelder personopplysninger, omfatter dette bare frivillig utlevering fra den berørte personen selv, og ikke fra en behandlingsansvarlig som innehar slike opplysninger (noe som ville ha krevd et spesifikt rettslig grunnlag i henhold til loven om vern av personopplysninger). Frivillig utleverte gjenstander godtas som bevismateriale i rettssaker bare dersom det ikke er noen rimelig tvil om at utleveringen har skjedd frivillig, noe det er opp til påtalemyndigheten å bevise. Se høyesteretts avgjørelse 2013Do11233 av 10. mars 2016.
([35]) Artikkel 308-2 i CPA.
([36]) Artikkel 321 i straffeloven.
([37]) Artikkel 3 i CPPA. Loven om militærdomstolen regulerer innsamlingen av opplysninger om militært personell og kan bare anvendes på sivile i et begrenset antall tilfeller (dersom militært personell og sivile begår en straffbar handling sammen, eller dersom en person begår en straffbar handling mot militæret, kan det for eksempel anlegges sak ved en militærdomstol, se artikkel 2 i loven om militærdomstolen). De generelle bestemmelsene om ransaking og beslaglegging svarer til dem i CPA, se for eksempel artikkel 146–149 og 153–156 i loven om militærdomstolen. Postforsendelser kan for eksempel bare samles inn dersom det er nødvendig i forbindelse med en etterforskning, og krever en kjennelse fra militærdomstolen. I den grad elektronisk kommunikasjon samles inn på, får begrensningene og garantiene i CPPA anvendelse.
([38]) Artikkel 2 nr. 1 i CPPA, det vil si «overføring eller mottak av alle typer lyd, ord, symboler eller bilder via kabel, trådløst, fiberkabel eller andre elektromagnetiske systemer, herunder telefon, e-post, medlemskapsinformasjonstjeneste, faks og personsøker».
([39]) Artikkel 2 nr. 7 og artikkel 3 nr. 2 i CPPA.
([40]) «Sensur» defineres som å «åpne post uten den berørte partens samtykke eller å innhente kunnskap om, ta opp eller holde tilbake innholdet på annen måte» (artikkel 2 nr. 6 i CPPA). «Avlytting» defineres som å «samle inn eller ta opp innhold i telekommunikasjon ved å lytte til eller lese av lyder, ord, symboler eller bilder i kommunikasjonen ved bruk av elektronisk og mekanisk utstyr uten den berørte partens samtykke eller å forstyrre overføringen og mottaket av kommunikasjonen» (artikkel 2 nr. 7 i CPPA).
([41]) Artikkel 2 nr. 11 i CPPA.

Ved CPPA er det fastsatt begrensninger og garantier for innsamling av begge typer opplysninger, og manglende overholdelse av flere av disse kravene er underlagt strafferettslige sanksjoner([42]).

2.2.2.2. Begrensninger og garantier for innsamling av kommunikasjonsinnhold (kommunikasjonsbegrensende tiltak)

Innsamling av kommunikasjonsinnhold kan bare skje som et supplerende middel for å lette en strafferettslig etterforskning (det vil si som en siste utvei), og det skal gjøres en innsats for å minimere inngripenen i borgernes rett til kommunikasjonshemmelighet([43]). I tråd med dette generelle prinsippet kan kommunikasjonsbegrensende tiltak bare anvendes dersom det er vanskelig å hindre at det begås en straffbar handling, pågripe en gjerningsperson eller innhente bevismateriale på annen måte([44]). Rettshåndhevende myndigheter som samler inn kommunikasjonsinnhold, skal slutte med dette umiddelbart når fortsatt tilgang ikke lenger anses for å være nødvendig, noe som sikrer at krenkingen av personvernet i forbindelse med kommunikasjon begrenses mest mulig([45]).

Videre kan kommunikasjonsbegrensende tiltak bare brukes når det er vektige grunner til å mistenke at visse alvorlige straffbare handlinger som er spesifikt oppført i CPPA, planlegges, begås eller er blitt begått. Dette omfatter opprør, narkotikarelaterte straffbare handlinger, straffbare handlinger der eksplosiver er involvert, og straffbare handlinger knyttet til nasjonal sikkerhet, diplomatiske forbindelser eller militærbaser og -installasjoner([46]). Et kommunikasjonsbegrensende tiltak skal være rettet mot spesifikke postforsendelser eller spesifikk telekommunikasjon som sendes eller mottas av den mistenkte, eller postforsendelser eller telekommunikasjon som sendes eller mottas av den mistenkte i en bestemt periode([47]).

Selv når disse kravene er oppfylt, kan innsamlingen av kommunikasjonsinnhold bare skje på grunnlag av en rettskjennelse. En påtalemyndighet kan særlig anmode domstolen om å tillate innsamling av kommunikasjonsinnhold som gjelder en mistenkt eller en person som er under etterforskning([48]). På samme måte kan kriminalpolitiet anmode en påtalemyndighet om tillatelse, og denne kan i neste omgang framsette en begjæring om rettskjennelse([49]). En begjæring om kjennelse skal framsettes skriftlig og skal inneholde spesifikke elementer. Den skal særlig inneholde 1) de vektige grunnene til å mistenke at en av de oppførte straffbare handlingene planlegges, begås eller er blitt begått, samt eventuell dokumentasjon som godtgjør at det umiddelbart (*prima facie*) er en grunn til mistanke, 2) de kommunikasjonsbegrensende tiltakene og tiltakenes mål, omfang, formål og varighet og 3) stedet der tiltakene vil bli gjennomført, og måten de vil bli gjennomført på([50]).

Dersom de rettslige kravene er oppfylt, kan retten gi skriftlig tillatelse til å gjennomføre kommunikasjonsbegrensende tiltak rettet mot den mistenkte eller personen som etterforskes([51]). I denne kjennelsen angis tiltakene og tiltakenes mål, omfang, varighet, stedet der de vil bli gjennomført, og måten de vil bli gjennomført på([52]).

Kommunikasjonsbegrensende tiltak kan bare gjennomføres i en periode på to måneder([53]). Dersom formålet med tiltakene oppnås før denne fristen, skal tiltakene innstilles umiddelbart. Dersom de nødvendige vilkårene derimot fortsatt er oppfylt, kan det innen fristen på to måneder inngis en anmodning om forlengelse av varigheten av de kommunikasjonsbegrensende tiltakene. En slik anmodning skal inneholde dokumentasjon som godtgjør at det foreligger en umiddelbar (*prima facie*) grunn til å forlenge tiltakene([54]). Forlengelsen kan ikke vare lenger enn ett år eller tre år for visse spesielt alvorlige straffbare handlinger (for eksempel knyttet til opprør, aggresjon utenfra, nasjonal sikkerhet)([55]).

Rettshåndhevende myndigheter kan kreve bistand fra kommunikasjonsoperatører ved å framlegge rettens skriftlige tillatelse for dem([56]). Kommunikasjonsoperatører skal samarbeide og oppbevare denne tillatelsen i sine registre([57]). De kan nekte å samarbeide når opplysningene om personen angitt i rettens skriftlige tillatelse (for eksempel personens telefonnummer) ikke er riktige. De skal ikke under noen omstendigheter utlevere passord som brukes til telekommunikasjon([58]).

([42]) Artikkel 16 og 17 i CPPA. Dette gjelder for eksempel innsamling uten kjennelse, manglende registerføring, unnlatelse av å innstille innsamlingen når en nødssituasjon opphører, eller manglende underretning av den berørte personen.
([43]) Artikkel 3 nr. 2 i CPPA.
([44]) Artikkel 5 nr. 1 i CPPA.
([45]) Artikkel 2 i gjennomføringsdekretet til CPPA.
([46]) Artikkel 5 nr. 1 i CPPA.
([47]) Artikkel 5 nr. 2 i CPPA.
([48]) Artikkel 6 nr. 1 i CPPA.
([49]) Artikkel 6 nr. 2 i CPPA.
([50]) Artikkel 6 nr. 4 i CPPA og artikkel 4 nr. 1 i gjennomføringsdekretet til CPPA.
([51]) Artikkel 6 nr. 5 og artikkel 6 nr. 8 i CPPA.
([52]) Artikkel 6 nr. 6 i CPPA.
([53]) Artikkel 6 nr. 7 i CPPA.
([54]) Artikkel 6 nr. 7 i CPPA.
([55]) Artikkel 6 nr. 8 i CPPA.
([56]) Artikkel 9 nr. 2 i CPPA.
([57]) Artikkel 15-2 i CPPA og artikkel 12 i gjennomføringsdekretet til CPPA.
([58]) Artikkel 9 nr. 4 i CPPA.

Enhver som gjennomfører kommunikasjonsbegrensende tiltak, eller som anmodes om å samarbeide, skal føre registre over formålene med tiltakene, gjennomføringen av dem, datoen for innledning av samarbeidet og målet([59]). Rettshåndhevende myndigheter som gjennomfører kommunikasjonsbegrensende tiltak, skal også føre registre med detaljerte opplysninger og oppnådde resultater([60]). Kriminalpolitiet skal gi disse opplysningene i form av en rapport til påtalemyndigheten når en etterforskning avsluttes([61]).

Når en påtalemyndighet reiser tiltale i en sak der det er brukt kommunikasjonsbegrensende tiltak, beslutter å ikke reise tiltale eller pågripe den aktuelle personen (det vil si at det ikke bare er snakk om utsatt rettsforfølgning), skal den underrette personen som er gjenstand for de kommunikasjonsbegrensende tiltakene, om at det er gjennomført kommunikasjonsbegrensende tiltak, hvem som har gjennomført dem, og varigheten av dem. Underretningen skal skje skriftlig senest 30 dager etter beslutningen([62]). Underretningen kan utsettes dersom det er sannsynlig at den vil utgjøre en alvorlig trussel mot den nasjonale sikkerheten eller forstyrre den offentlige sikkerheten og ordenen, eller dersom det er sannsynlig at den vil føre til vesentlig skade på andres liv og legeme([63]). Dersom påtalemyndigheten eller kriminalpolitiet ønsker å utsette underretningen, skal det innhentes godkjenning fra lederen for det lokale statsadvokatkontoret([64]). Når grunnene til utsettelsen ikke lenger foreligger, skal underretningen gis senest 30 dager fra det tidspunktet([65]).

I CPPA er det også fastsatt en spesifikk prosedyre for innsamling av kommunikasjonsinnhold i nødssituasjoner. Rettshåndhevende myndigheter kan samle inn kommunikasjonsinnhold dersom det foreligger en overhengende fare for planlegging eller gjennomføring av organisert kriminalitet eller andre alvorlige straffbare handlinger som direkte kan forårsake dødsfall eller alvorlig skade, og det foreligger en nødssituasjon som gjør det umulig å følge den vanlige prosedyren (som fastsatt over)([66]). I en slik nødssituasjon kan politi eller påtalemyndighet treffe kommunikasjonsbegrensende tiltak uten at det på forhånd er innhentet rettskjennelse, men skal inngi en begjæring om rettskjennelse umiddelbart etter iverksettelsen. Dersom den rettshåndhevende myndigheten ikke innhenter rettskjennelsen senest 36 timer etter tidspunktet for iverksettelsen av hastetiltakene, skal innsamlingen innstilles umiddelbart og de innsamlede opplysningene som regel tilintetgjøres([67]). Polititjenestemenn som gjennomfører overvåking i nødssituasjoner, gjør dette under en påtalemyndighets kontroll, og dersom det ikke er mulig å motta instruksjoner fra påtalemyndigheten på forhånd på grunn av behovet for å handle raskt, skal politiet innhente godkjenning fra påtalemyndigheten umiddelbart etter at iverksettingen er startet([68]). Reglene beskrevet over for underretning av personen får også anvendelse på innsamlingen av kommunikasjonsinnhold i nødssituasjoner.

Innsamling av opplysninger i nødssituasjoner skal alltid skje i samsvar med en «erklæring om sensur/avlytting i nødssituasjoner», og myndigheten som foretar innsamlingen, skal føre et register over eventuelle hastetiltak([69]). Anmodningen til en domstol om tillatelse til hastetiltak skal ledsages av et skriftlig dokument med angivelse av de nødvendige kommunikasjonsbegrensende tiltakene, målet, emnet, omfanget, varigheten, gjennomføringsstedet, metoden og en redegjørelse for hvordan de relevante kommunikasjonsbegrensende tiltakene oppfyller artikkel 5 nr. 1 i CPPA([70]), sammen med underlagsdokumenter.

Dersom hastetiltakene avsluttes etter kort tid, noe som utelukker innhenting av rettskjennelse (for eksempel dersom den mistenkte pågripes umiddelbart etter at avlyttingen er startet, og som derfor stopper), skal lederen for vedkommende statsadvokatkontor inngi en melding om hastetiltak til vedkommende domstol([71]). I meldingen angis formålet, målet, omfanget, varigheten, gjennomføringsstedet og innsamlingsmetoden samt grunnene til at det ikke er framsatt en begjæring om rettskjennelse([72]). Denne meldingen gir den mottakende domstolen mulighet til å undersøke om innsamlingen er lovlig, og den skal registreres i et register over meldinger om hastetiltak.

([59]) Artikkel 9 nr. 3 i CPPA.
([60]) Artikkel 18 nr. 1 i gjennomføringsdekretet til CPPA.
([61]) Artikkel 18 nr. 2 i gjennomføringsdekretet til CPPA.
([62]) Artikkel 9-2 nr. 1 i CPPA.
([63]) Artikkel 9-2 nr. 4 i CPPA.
([64]) Artikkel 9-2 nr. 5 i CPPA.
([65]) Artikkel 9-2 nr. 6 i CPPA.
([66]) Artikkel 8 nr. 1 i CPPA.
([67]) Artikkel 8 nr. 2 i CPPA.
([68]) Artikkel 8 nr. 3 i CPPA og artikkel 16 nr. 3 i gjennomføringsdekretet til CPPA.
([69]) Artikkel 8 nr. 4 i CPPA.
([70]) Det vil si at det er vektige grunner til å mistenke at visse alvorlige straffbare handlinger planlegges, begås eller er blitt begått, og det er umulig å hindre at det begås en straffbar handling, pågripe gjerningspersonen eller samle inn bevismateriale på annen måte.
([71]) Artikkel 8 nr. 5 i CPPA.
([72]) Artikkel 8 nr. 6–7 i CPPA.

Som et generelt krav kan kommunikasjonsinnhold som oppnås gjennom kommunikasjonsbegrensende tiltak på grunnlag av CPPA, bare brukes til å etterforske, rettsforfølge eller hindre de spesifikke formene for straffbare forhold som er nevnt over, i disiplinærsaker i forbindelse med disse straffbare forholdene, i forbindelse med erstatningskrav reist av en part i kommunikasjonen eller dersom dette er tillatt i henhold til annen lovgivning([73]).

Det gjelder særlige garantier ved innsamling av telekommunikasjon som overføres via internett([74]). Slike opplysninger kan bare brukes til å etterforske de alvorlige straffbare handlingene som er angitt i artikkel 5 nr. 1 i CPPA. For å kunne lagre opplysninger må det innhentes godkjenning fra den domstolen som godkjente de kommunikasjonsbegrensende tiltakene([75]). En anmodning om lagring skal inneholde informasjon om de kommunikasjonsbegrensende tiltakene, et sammendrag av resultatene av tiltakene, grunnene til lagringen (sammen med dokumentasjon) og om den telekommunikasjonen som skal lagres([76]). Dersom det ikke foreligger en slik anmodning, skal den innsamlede telekommunikasjonen slettes senest 14 dager etter at de kommunikasjonsbegrensende tiltakene er avsluttet([77]). Dersom en anmodning avvises, skal telekommunikasjonen tilintetgjøres innen sju dager([78]). Dersom telekommunikasjonen slettes, skal det innen sju dager inngis en rapport til den domstolen som godkjente de kommunikasjonsbegrensende tiltakene, med angivelse av årsaken til slettingen og nærmere opplysninger og tidspunktet for dette.

Mer generelt vil opplysninger som er innhentet på ulovlig vis ved bruk av kommunikasjonsbegrensende tiltak, ikke godtas som bevismateriale i rettssaker eller disiplinærsaker([79]). I henhold til CPPA er det dessuten forbudt for personer som treffer kommunikasjonsbegrensende tiltak, å utlevere konfidensielle opplysninger som er innhentet i forbindelse med gjennomføringen av slike tiltak, og å bruke de innhentede opplysningene til å skade omdømmet til personene som omfattes av tiltakene([80]).

2.2.2.3. Begrensninger og garantier for innsamling av kommunikasjonsbekreftelsesdata

På grunnlag av CPPA kan rettshåndhevende myndigheter anmode teleoperatører om å framlegge kommunikasjonsbekreftelsesdata når det er nødvendig for å gjennomføre en etterforskning eller iverksette en dom([81]). I motsetning til det som er tilfellet ved innsamling av kommunikasjonsinnhold, er muligheten til å samle inn kommunikasjonsbekreftelsesdata ikke begrenset til visse spesifikke straffbare handlinger. Som med kommunikasjonsinnhold krever innsamlingen av kommunikasjonsbekreftelsesdata imidlertid skriftlig forhåndstillatelse fra en domstol på de samme vilkårene som er beskrevet over([82]). Dersom saken haster og dette gjør det umulig å innhente en rettskjennelse, kan kommunikasjonsbekreftelsesdata samles inn uten kjennelse, da skal kjennelsen innhentes umiddelbart etter at det er anmodet om dataene, og videresendes til telekommunikasjonsleverandøren([83]). Dersom det ikke innhentes en kjennelse i ettertid, skal de innsamlede opplysningene tilintetgjøres([84]).

Påtalemyndigheten, kriminalpolitiet og domstolene skal føre registre over anmodninger som gjelder kommunikasjonsbekreftelsesdata([85]). Telekommunikasjonsleverandører skal dessuten to ganger i året rapportere om utleveringen av kommunikasjonsbekreftelsesdata til ministeren for vitenskap og IKT og lagre disse opplysningene i sju år fra den datoen dataene ble utlevert([86]).

Enkeltpersoner underrettes i prinsippet om at det er blitt samlet inn kommunikasjonsbekreftelsesdata([87]). Tidspunktet for en slik underretning avhenger av omstendighetene rundt etterforskningen([88]). Når det er truffet beslutning om å (ikke) rettsforfølge, skal underretningen skje innen 30 dager. Dersom tiltalen derimot oppheves midlertidig, skal underretningen skje senest 30 dager ett år etter at en slik beslutning er truffet. I alle tilfeller skal underretningen skje senest 30 dager ett år etter at opplysningene er samlet inn.

([73]) Artikkel 12 i CPPA.
([74]) Artikkel 12-2 i CPPA.
([75]) Påtalemyndigheten eller polititjenestemannen som gjennomfører de kommunikasjonsbegrensende tiltakene, skal velge den telekommunikasjonen som skal lagres, senest 14 dager etter at tiltakene er avsluttet, og anmode om domstolsgodkjenning (når det gjelder en polititjenestemann, skal anmodningen inngis til en påtalemyndighet, som deretter videresender den til domstolen), se artikkel 12-2 nr. 1 og 2 i CPPA.
([76]) Artikkel 12-2 nr. 3 i CPPA.
([77]) Artikkel 12-2 nr. 5 i CPPA.
([78]) Artikkel 12-2 nr. 5 i CPPA.
([79]) Artikkel 4 i CPPA.
([80]) Artikkel 11 nr. 2 i gjennomføringsdekretet til CPPA.
([81]) Artikkel 13 nr. 1 i CPPA.
([82]) Artikkel 13 og 6 i CPPA.
([83]) Artikkel 13 nr. 2 i CPPA. Som med kommunikasjonsbegrensende hastetiltak skal det utarbeides et dokument med nærmere opplysninger om saken (den mistenkte, tiltakene som skal treffes, den mistenkte straffbare handlingen og årsaken til at saken haster). Se artikkel 37 nr. 5 i gjennomføringsdekretet til CPPA.
([84]) Artikkel 13 nr. 3 i CPPA.
([85]) Artikkel 13 nr. 5 og 6 i CPPA.
([86]) Artikkel 13 nr. 7 i CPPA.
([87]) Se artikkel 13-3 nr. 7 sammenholdt med artikkel 9-2 i CPPA.
([88]) Artikkel 13-3 nr. 1 i CPPA.

Underretningen kan utsettes dersom det er sannsynlig at den vil 1) sette den nasjonale sikkerheten og den offentlige sikkerheten og ordenen i fare, 2) forårsake død eller kroppsskade, 3) hindre en rettferdig rettergang (for eksempel føre til ødeleggelse av bevismateriale eller trusler mot vitner) eller 4) ærekrenke den mistenkte, ofrene eller andre personer med tilknytning til saken eller krenke deres personvern([89]). Underretning av en av de ovennevnte grunnene krever tillatelse fra lederen for vedkommende lokale statsadvokatkontor([90]). Når grunnene til utsettelsen ikke lenger foreligger, skal underretningen gis senest 30 dager fra det tidspunktet([91]).

Underrettede personer kan inngi en skriftlig anmodning til påtalemyndigheten eller kriminalpolitiet angående grunnene til innsamlingen av kommunikasjonsbekreftelsesdataene([92]). Da skal påtalemyndigheten eller kriminalpolitiet gi en skriftlig begrunnelse senest 30 dager etter å ha mottatt anmodningen, med mindre en av de ovennevnte grunnene (unntak for utsettelse av underretning) får anvendelse([93]).

2.2.3. *Teleoperatørers frivillige utlevering av opplysninger*

I henhold til artikkel 83 nr. 3 i TBA kan teleoperatører frivillig etterkomme en anmodning (inngitt for å støtte en straffesak, etterforskning eller iverksetting av en dom) fra en domstol, påtalemyndighet eller lederen for et etterforskningsorgan om å utlevere «kommunikasjonsopplysninger». I TBA omfatter «kommunikasjonsopplysninger» brukernes navn, folkeregisternummer, adresse og telefonnummer, datoene for brukernes tegning eller oppsigelse av sitt abonnement og brukeridentifikasjonskoder (det vil si koder som brukes for å identifisere den rettmessige brukeren av datasystemer eller kommunikasjonsnettverk)([94]). I forbindelse med TBA er det bare personer som inngår avtaler om tjenester direkte med en sørkoreansk telekommunikasjonsleverandør, som anses som brukere([95]). Det gjør at situasjoner der EU-borgere som har fått sine opplysninger overført til Republikken Korea, vil bli ansett som brukere i henhold til TBA, sannsynligvis vil være svært begrenset, ettersom disse personene normalt ikke inngår en direkte avtale med en sørkoreansk teleoperatør.

Anmodninger om innhenting av kommunikasjonsopplysninger på grunnlag av TBA må inngis skriftlig med en angivelse av begrunnelsen for anmodningen, lenken til den relevante brukeren og omfanget av dataene det bes om([96]). Dersom saken haster og det derfor ikke er mulig å inngi en skriftlig anmodning, skal den skriftlige anmodningen inngis så snart grunnen til at saken haster, ikke lenger foreligger([97]). Teleoperatører som etterkommer anmodninger om utlevering av kommunikasjonsopplysninger, skal føre registre over utleveringen av kommunikasjonsopplysninger og tilknyttet materiale, for eksempel den skriftlige anmodningen([98]). Teleoperatører skal dessuten rapportere om utleveringen av kommunikasjonsopplysninger til ministeren for vitenskap og IKT to ganger i året([99]).

Teleoperatører plikter ikke å etterkomme anmodninger om utlevering av kommunikasjonsopplysninger på grunnlag av TBA. Operatøren må derfor vurdere hver anmodning i lys av gjeldende krav til vern av opplysninger i henhold til PIPA. En teleoperatør skal særlig ta hensyn til den registrertes interesser og kan ikke utlevere opplysningene dersom det er sannsynlig at det vil krenke vedkommendes eller en tredjeparts interesser urettmessig([100]). Den registrerte skal i henhold til melding 2021-1 om utfyllende regler for fortolkning og anvendelse av loven om vern av personopplysninger i tillegg underrettes om utleveringen. I unntakstilfeller kan en slik underretning utsettes, særlig dersom og så lenge underretningen vil kunne bringe en pågående strafferettslig etterforskning i fare eller det er sannsynlig at det vil skade en annen persons liv eller legeme, dersom disse rettighetene eller interessene klart går foran den registrertes rettigheter ([101]).

I 2016 bekreftet høyesterett at teleoperatøres frivillige utlevering av kommunikasjonsopplysninger uten kjennelse på grunnlag av TBA ikke i seg selv krenker den retten brukeren av telekommunikasjonstjenesten har til selvbestemmelse over opplysninger. Høyesterett presiserte samtidig at det vil foreligge en slik krenking dersom det er åpenbart at det anmodende organet har misbrukt sin myndighet til å anmode om utlevering av kommunikasjonsopplysninger og dermed har krenket den registrertes eller en tredjeparts interesser([102]). Mer generelt skal rettshåndhevende myndigheters anmodninger om frivillig utlevering være i samsvar med prinsippene om lovlighet, nødvendighet og forholdsmessighet som følger av den sørkoreanske forfatningen (artikkel 12 nr. 1 og artikkel 37 nr. 2).

([89]) Artikkel 13-3 nr. 2 i CPPA.
([90]) Artikkel 13-3 nr. 3 i CPPA.
([91]) Artikkel 13-3 nr. 4 i CPPA.
([92]) Artikkel 13-3 nr. 5 i CPPA.
([93]) Artikkel 13-3 nr. 6 i CPPA.
([94]) Artikkel 83 nr. 3 i TBA.
([95]) Artikkel 2 nr. 9 i TBA.
([96]) Artikkel 83 nr. 4 i TBA.
([97]) Artikkel 83 nr. 4 i TBA.
([98]) Artikkel 83 nr. 5 i TBA.
([99]) Artikkel 83 nr. 6 i TBA.
([100]) Artikkel 18 nr. 2 i PIPA.
([101]) Melding 2021-1 fra PIPC om utfyllende regler for fortolkning og anvendelse av loven om vern av personopplysninger, avsnitt III nr. 2 punkt iii).
([102]) Høyesteretts avgjørelse 2012Da105482 av 10. mars 2016.

2.3. **Tilsyn**

Tilsynet med de strafferettshåndhevende myndighetene skjer ved hjelp av forskjellige mekanismer, både internt og via eksterne organer.

2.3.1. *Egenrevisjon*

I samsvar med loven om revisjoner i den offentlige sektor oppmuntres offentlige myndigheter til å opprette et internt egenrevisjonsorgan som blant annet skal ha som oppgave å foreta lovlighetskontroll([103]). Lederne for slike revisjonsorganer skal i størst mulig omfang garanteres uavhengighet([104]). Mer spesifikt skal de hentes utenfor den relevante myndigheten (for eksempel tidligere dommere eller professorer) og utnevnes for en periode på to til fem år og kan bare avsettes når det er velbegrunnet (for eksempel dersom vedkommende på grunn av psykisk eller fysisk sykdom eller disiplinære tiltak ikke er i stand til å ivareta sine oppgaver)([105]). Revisorer utnevnes også på grunnlag av spesifikke vilkår fastsatt i loven([106]). Revisjonsrapportene kan inneholde anbefalinger eller anmodninger om erstatning eller korrigering samt irettesettelser og anbefalinger eller anmodninger om disiplinære tiltak([107]). De meddeles lederen for den offentlige myndigheten som er gjenstand for revisjonen, og revisjons- og granskingsutvalget (se avsnitt 2.3.2) senest 60 dager etter at revisjonen er avsluttet([108]). Den berørte myndigheten skal gjennomføre de nødvendige tiltakene og rapportere om resultatene til revisjons- og granskingsutvalget([109]). Resultatene av revisjonen offentliggjøres som regel([110]). Ved nekting av å gjennomføre eller hindring av en egenrevisjon kan det ilegges administrative bøter([111]). På området strafferettslig håndheving har den nasjonale politimyndigheten innført et generalinspektørsystem for å håndtere internrevisjoner, herunder med hensyn til mulig krenking av menneskerettighetene, for å overholde ovennevnte lovgivning([112]).

2.3.2. *Revisjons- og granskingsutvalget*

Revisjons- og granskingsutvalget (Board of Audit and Inspection, heretter kalt «BAI») kan granske offentlige myndigheters aktiviteter og på grunnlag av slike granskinger utstede anbefalinger, anmode om disiplinære tiltak eller anmelde forhold([113]). BAI er opprettet under Republikken Koreas president, men har en uavhengig status med hensyn til oppgavene det skal utføre([114]). I henhold til loven om opprettelse av BAI skal BAI dessuten ha en størst mulig grad av uavhengighet med hensyn til utnevnelse, avsettelse og organisering av sitt personale og utarbeiding av sitt budsjett([115]). BAIs leder utnevnes av presidenten med nasjonalforsamlingens samtykke([116]). De seks resterende medlemmene utnevnes av presidenten på anbefaling fra lederen for en periode på fire år([117]). Utvalgsmedlemmene (herunder lederen) skal inneha spesifikke lovbestemte kvalifikasjoner([118]) og kan bare avsettes dersom det reises tiltale eller i tilfelle fengselsstraff eller manglende evne til å ivareta egne oppgaver som følge av langvarig svekket fysisk eller psykisk funksjonsevne([119]). Det er dessuten forbudt for utvalgsmedlemmene å delta i politiske aktiviteter og samtidig inneha verv i nasjonalforsamlingen, forvaltningsorganer, organisasjoner som er underlagt BAIs revisjon og gransking, eller andre lønnede verv eller stillinger([120]).

BAI foretar en generell revisjon én gang i året, men kan også foreta spesifikke revisjoner ved spørsmål av særlig interesse. BAI kan under en gransking anmode om at det framlegges dokumenter, og om at enkeltpersoner skal være til stede([121]). Som en del av en revisjon gransker BAI statens inntekter og utgifter, men fører også tilsyn med at offentlige myndigheter og offentlige

([103]) Artikkel 3 og 5 i loven om revisjoner i den offentlige sektor.
([104]) Artikkel 7 i loven om revisjoner i den offentlige sektor.
([105]) Artikkel 8–11 i loven om revisjoner i den offentlige sektor.
([106]) Artikkel 16 ff. i loven om revisjoner i den offentlige sektor.
([107]) Artikkel 23 nr. 2 i loven om revisjoner i den offentlige sektor.
([108]) Artikkel 23 nr. 1 i loven om revisjoner i den offentlige sektor.
([109]) Artikkel 23 nr. 3 i loven om revisjoner i den offentlige sektor.
([110]) Artikkel 26 i loven om revisjoner i den offentlige sektor.
([111]) Artikkel 41 i loven om revisjoner i den offentlige sektor.
([112]) Se særlig avdelingene under generaldirektøren for revisjon og inspeksjon: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Artikkel 24 og artikkel 31-35 i loven om revisjons- og granskingsutvalget (Board of Audit and Inspection Act, heretter kalt «BAI-loven»).
([114]) Artikkel 2 nr. 1 i BAI-loven.
([115]) Artikkel 2 nr. 2 i BAI-loven.
([116]) Artikkel 4 nr. 1 i BAI-loven.
([117]) Artikkel 5 nr. 1 og artikkel 6 i BAI-loven.
([118]) For eksempel ha arbeidet som dommer, statsadvokat eller advokat i minst ti år, som offentlig tjenestemann eller professor eller i en høyere stilling ved et universitet i minst åtte år eller ha arbeidet i minst ti år i et børsnotert selskap eller statsfinansiert institusjon (herav minst fem år som administrerende direktør), se artikkel 7 i BAI-loven.
([119]) Artikkel 8 i BAI-loven.
([120]) Artikkel 9 i BAI-loven.
([121]) Se for eksempel artikkel 27 i BAI-loven.

tjenestemenn generelt overholder sine forplikter, med henblikk på å forbedre måten den offentlige forvaltningen fungerer på([122]). Tilsynet omfatter derfor mer enn bare budsjettmessige aspekter, blant annet lovlighetskontroll.

2.3.3. *Nasjonalforsamlingen*

Nasjonalforsamlingen kan undersøke og granske offentlige myndigheter([123]). I forbindelse med en undersøkelse eller gransking kan nasjonalforsamlingen anmode om utlevering av dokumenter og pålegge vitner å møte([124]). Enhver som avgir falsk forklaring i forbindelse med nasjonalforsamlingens undersøkelser kan ilegges strafferettslige sanksjoner (fengsel i opptil ti år)([125]). Prosessen og resultatene av granskingene kan offentliggjøres([126]). Dersom nasjonalforsamlingen fastslår at det har funnet sted ulovlige eller urettmessige aktiviteter, kan den anmode om at den relevante offentlige myndigheten treffer korrigerende tiltak, herunder gir erstatning, treffer disiplinære tiltak og forbedrer sine interne prosedyrer([127]). Etter en slik anmodning skal myndigheten uten opphold handle og rapportere resultatet til nasjonalforsamlingen([128]).

2.3.4. *Kommisjonen for vern av personopplysninger*

Kommisjonen for vern av personopplysninger (Personal Information Protection Commission, heretter kalt «PIPC») fører tilsyn med strafferettshåndhevende myndigheters behandling av personopplysninger i samsvar med PIPA. I henhold til artikkel 7-8 nr. 3 og 4 og artikkel 7-9 nr. 5 i PIPA omfatter PIPCs tilsyn også mulige overtredelser av reglene for begrensning og garantier i forbindelse med innsamling av personopplysninger, herunder reglene i de spesifikke lovene om innsamling av (elektronisk) bevismateriale med henblikk på strafferettslig håndheving (se avsnitt 2.2). Med hensyn til kravene i artikkel 3 nr. 1 i PIPA om lovlig og rettferdig innsamling av personopplysninger utgjør en slik overtredelse også en overtredelse av PIPA, noe som gjør det mulig for PIPC å gjennomføre undersøkelser og treffe korrigerende tiltak([129]).

PIPC har ved utøvelsen av sin tilsynsfunksjon tilgang til all relevant informasjon([130]). PIPC kan gi råd til rettshåndhevende myndigheter om å forbedre beskyttelsesnivået for personopplysninger i forbindelse med behandlingsaktiviteter, treffe korrigerende tiltak (for eksempel innstille behandlingen eller treffe nødvendige tiltak for å verne personopplysningene) eller gi myndighetene råd om å treffe disiplinære tiltak([131]). Det er fastsatt strafferettslige sanksjoner for visse overtredelser av PIPA, for eksempel ulovlig bruk eller utlevering av personopplysninger til tredjeparter eller ulovlig behandling av sensitive opplysninger([132]). I denne forbindelse kan PIPC henvise saken til vedkommende etterforskningsorgan (herunder påtalemyndighet)([133]).

2.3.5. *Den nasjonale menneskerettighetskommisjonen*

Den nasjonale menneskerettighetskommisjonen (National Human Rights Commission, heretter kalt «NHRC») er et uavhengig organ som har som oppgave å verne og fremme grunnleggende rettigheter([134]), og som har myndighet til å undersøke og avhjelpe overtredelser av forfatningens artikkel 10–22, som omfatter retten til personvern og personvern i forbindelse med korrespondanse. NHRC består av elleve kommisjonsmedlemmer som utnevnes etter innstilling fra nasjonalforsamlingen (fire), presidenten (fire) og høyesterettsjustitiarius (tre)([135]). For å bli utnevnt må et kommisjonsmedlem 1) ha arbeidet i minst ti år ved et universitet eller et godkjent forskningsinstitutt minst som assisterende professor, 2) ha arbeidet som dommer, statsadvokat eller advokat i minst ti år, 3) ha deltatt i menneskerettighetsaktiviteter i minst ti år (for eksempel for en ideell ikke-statlig organisasjon eller internasjonal organisasjon) eller 4) være blitt anbefalt av sivilsamfunnsgrupper([136]). Lederen utnevnes av

([122]) Artikkel 20 og 24 i BAI-loven.
([123]) Artikkel 128 i loven om nasjonalforsamlingen og artikkel 2, 3 og 15 i loven om gransking og undersøkelse av statsforvaltningen. Dette omfatter årlige inspeksjoner av offentlige anliggender generelt og gransking av spesifikke saker.
([124]) Artikkel 10 nr. 1 i loven om gransking og undersøkelse av statsforvaltningen. Se også artikkel 128 og 129 loven om nasjonalforsamlingen.
([125]) Artikkel 14 i loven om vitneutsagn, vurdering osv. for nasjonalforsamlingen.
([126]) Artikkel 12-2 i loven om gransking og undersøkelse av statsforvaltningen.
([127]) Artikkel 16 nr. 2 i loven om gransking og undersøkelse av statsforvaltningen.
([128]) Artikkel 16 nr. 3 i loven om gransking og undersøkelse av statsforvaltningen.
([129]) Se PIPCs melding 2021-1 om utfyllende regler for fortolkning og anvendelse av loven om vern av personopplysninger.
([130]) Artikkel 63 i PIPA.
([131]) Artikkel 61 nr. 2, artikkel 65 nr. 1, artikkel 65 nr. 2 og artikkel 64 nr. 4 i PIPA.
([132]) Artikkel 70–74 i PIPA.
([133]) Artikkel 65 nr. 1 i PIPA.
([134]) Artikkel 1 i loven om menneskerettighetskommisjonen (Human Rights Commission Act, heretter kalt «NHRC-loven»).
([135]) Artikkel 5 nr. 1 og 2 i NHRC-loven.
([136]) Artikkel 5 nr. 3 i NHRC-loven.

presidenten blant kommisjonsmedlemmene, og utnevnelsen skal bekreftes av nasjonalforsamlingen([137]). Kommisjonsmedlemmene (herunder lederen) utnevnes for en periode på tre år som kan forlenges, og kan bare avsettes dersom de idømmes fengselsstraff eller ikke lenger er i stand til å utføre sine oppgaver på grunn av langvarig svekket fysisk eller psykisk funksjonsevne (i så fall skal to tredeler av kommisjonsmedlemmene være enige i avsettelsen)([138]). Det er forbudt for kommisjonsmedlemmene å samtidig inneha verv i nasjonalforsamlingen, i lokale råd eller hos en statlig eller lokal myndighet (som offentlig tjenestemann)([139]).

NHRC kan innlede en undersøkelse på eget initiativ eller på grunnlag av anmodninger fra enkeltpersoner. Som ledd i undersøkelsen kan NHRC anmode at det framlegges relevant materiale, gjennomføre granskinger og innkalle enkeltpersoner for å avgi vitneforklaring([140]). Etter en undersøkelse kan NHRC utstede anbefalinger for å bedre eller korrigere spesifikke strategier og praksis og kan offentliggjøre dem([141]). Offentlige myndigheter skal underrette NHRC om en plan for å gjennomføre slike anbefalinger senest 90 dager etter å ha mottatt dem([142]). Dersom anbefalingene ikke etterkommes, skal den berørte myndigheten dessuten underrette kommisjonen om dette([143]). NHRC kan deretter underrette nasjonalforsamlingen om at anbefalingene ikke etterkommes, og/eller offentliggjøre dette. Offentlige myndigheter etterkommer generelt sett NHRCs anbefalinger og har et sterkt insitament til å gjøre det, ettersom gjennomføringen er blitt vurdert å være en del av den generelle evalueringen som kontoret for samordning av regjeringens politikk har foretatt under myndigheten til statsministerens kontor.

2.4. **Individuell prøvings-/klageadgang**

2.4.1. *Prøvingsmekanismer i henhold til PIPA*

Enkeltpersoner kan utøve sin rett til innsyn i og til retting og sletting og til å få innstilt behandlingen i henhold til PIPA av personopplysninger som behandles av strafferettshåndhevende myndigheter. Det kan anmodes om innsyn direkte fra den relevante myndigheten eller indirekte via PIPC([144]). Vedkommende myndighet kan begrense eller nekte innsyn bare dersom dette er fastsatt ved lov, eller dersom det er sannsynlig at det vil skade en tredjepersons liv eller legeme eller urettmessig krenke en annen persons eiendom eller andre interesser (det vil si dersom den andre personens interesser veier tyngre enn interessene til enkeltpersonene som framsetter anmodningen)([145]). Dersom en anmodning om innsyn avslås, skal den aktuelle personen underrettes om grunnene til dette og om hvordan det kan klages på beslutningen([146]). En anmodning om retting eller sletting kan også avslås dersom dette er fastsatt i annen lovgivning, da skal den aktuelle personen underrettes om grunnene til dette og muligheten for å klage([147]).

Enkeltpersoner kan klage til PIPC, herunder via personverntelefontjenesten som drives av Republikken Koreas byrå for internett og sikkerhet([148]). Enkeltpersoner kan dessuten få adgang til mekling via utvalget for tvisteløsning i forbindelse med personopplysninger([149]). Disse rettsmidlene er tilgjengelige både ved mulige overtredelser av reglene i spesifikke lover der det er fastsatt særlige begrensninger og garantier for innsamling av personopplysninger (avsnitt 2.2), og i PIPA. Enkeltpersoner kan dessuten bestride PIPCs beslutninger eller unnlatelse av å handle i henhold til forvaltningsprosessloven (se avsnitt 2.4.3).

([137]) Artikkel 5 nr. 5 i NHRC-loven.
([138]) Artikkel 7 nr. 1 og artikkel 8 i NHRC-loven.
([139]) Artikkel 10 i NHRC-loven.
([140]) Artikkel 36 i NHRC-loven. I henhold til lovens artikkel 36 nr. 7 kan utlevering av materiale eller gjenstander avslås dersom det er fare for at det vil gå ut over statlige konfidensielle forhold som kan ha en vesentlig innvirkning på statens sikkerhet eller diplomatiske forbindelser, eller utgjøre en alvorlig hindring for en strafferettslig etterforskning eller verserende rettssak. I slike tilfeller kan kommisjonen anmode lederen for det relevante organet (som skal etterkomme anmodningen i god tro) om ytterligere informasjon dersom det er nødvendig for å kunne avgjøre om avslaget på utleveringen av informasjon er begrunnet.
([141]) Artikkel 25 nr. 1 i NHRC-loven.
([142]) Artikkel 25 nr. 3 i NHRC-loven.
([143]) Artikkel 25 nr. 4 i NHRC-loven.
([144]) Artikkel 35 nr. 2 i PIPA.
([145]) Artikkel 35 nr. 4 i PIPA.
([146]) Artikkel 42 nr. 2 i gjennomføringsdekretet til PIPA.
([147]) Artikkel 36 nr. 1–2 i PIPA og artikkel 43 nr. 3 i gjennomføringsdekretet til PIPA.
([148]) Artikkel 62 i PIPA.
([149]) Artikkel 40–50 i PIPA og artikkel 48-2 til 57 i gjennomføringsdekretet til PIPA.

2.4.2. *Klageadgang ved den nasjonale menneskerettighetskommisjonen*

NHRC behandler klager fra enkeltpersoner (både sørkoreanske statsborgere og fremmede borgere) som gjelder krenking av menneskerettighetene begått av offentlige myndigheter([150]). Det er intet krav om søksmålskompetanse for personer som ønsker å klage til NHRC([151]). Som følge av dette vil NHRC behandle klagen, selv om den berørte personen ikke kan påvise en faktisk skade på tidspunktet for gjennomgåelsen av om klagen kan behandles. Når det gjelder innsamling av personopplysninger for formål knyttet til strafferettslig håndheving, plikter en person derfor ikke å påvise at sørkoreanske offentlige myndigheter rent faktisk har fått tilgang til vedkommendes personopplysninger, for at NHRC skal kunne behandle klagen. En enkeltperson kan også anmode om å få avgjort klagesaken gjennom mekling([152]).

For å undersøke en klage kan NHRC bruke sin undersøkelsesmyndighet, herunder ved å anmode om å få framlagt relevant materiale, foreta inspeksjoner eller innkalle enkeltpersoner for å avgi vitneforklaring([153]). Dersom undersøkelsen viser at det har skjedd en overtredelse av relevante lover, kan NHRC anbefale at det gjennomføres tiltak, eller at relevante lover, institusjoner, retningslinjer eller praksis korrigeres eller forbedres([154]). Foreslåtte tiltak kan omfatte mekling, opphør av krenkingen av menneskerettighetene, skadeserstatning og tiltak for å hindre at de samme eller lignende overtredelser gjentar seg([155]). Ved ulovlig innsamling av personopplysninger i henhold til gjeldende regler kan de korrigerende tiltakene omfatte sletting av personopplysningene som er samlet inn. NHRC kan vedta hastetiltak dersom det anses som svært sannsynlig at overtredelsen vil fortsette, og dersom det anses som sannsynlig at det vil oppstå skade som er vanskelig å utbedre dersom det ikke gripes inn([156]).

NHRC har ikke tvangsmyndighet, men NHRCs beslutninger (for eksempel en beslutning om ikke å fortsette undersøkelsen av en klage)([157]) og anbefalinger kan bringes inn for de sørkoreanske domstolene i henhold til forvaltningsprosessloven (se avsnitt 2.4.3 nedenfor)([158]). Dersom NHRCs konklusjoner viser at personopplysningene er blitt samlet inn ulovlig av en offentlig myndighet, kan en person anlegge sak mot denne offentlige myndigheten ved de sørkoreanske domstolene, for eksempel ved å bestride innsamlingen i henhold til forvaltningsprosessloven, inngi en forfatningsmessig klage i henhold til loven om forfatningsdomstolen eller søke om skadeserstatning i henhold til loven om statlig erstatning (se avsnitt 2.4.3 nedenfor).

2.4.3. *Rettslig prøving*

Enkeltpersoner kan påberope seg begrensningene og garantiene beskrevet i forrige avsnitt for å få sin sak prøvd ved de sørkoreanske domstolene på forskjellige måter.

For det første kan den berørte personen og vedkommendes advokat i samsvar med CPA være til stede når en kjennelse om ransaking eller beslaglegging gjennomføres, og kan derfor gjøre innsigelse på tidspunktet for gjennomføring av kjennelsen([159]). CPA inneholder dessuten en såkalt «kvasiklage»-mekanisme som gir enkeltpersoner mulighet til å anmode vedkommende domstol om å annullere eller endre en disposisjon som en påtalemyndighet eller politiet har truffet om en beslaglegging([160]). Dette gjør det mulig for enkeltpersoner å bestride tiltakene som er truffet for å gjennomføre en kjennelse om beslaglegging.

([150]) Selv om det i artikkel 4 i NHRC-loven vises til statsborgere og utlendinger bosatt i Republikken Korea skal begrepet «bosatt» ses i sammenheng med begrepet «jurisdiksjon» og ikke «territorium». Dersom de grunnleggende rettighetene til en utlending bosatt utenfor Republikken Korea krenkes av nasjonale institusjoner i Republikken Korea, kan den aktuelle personen derfor klage til NHRC. Se for eksempel det aktuelle spørsmålet på NHRCs side med vanlige spørsmål på https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Dette vil være tilfellet dersom sørkoreanske offentlige myndigheter har ulovlig tilgang til en utlendings personopplysninger som er overført til Republikken Korea.

([151]) En klage skal i prinsippet inngis innen et år etter overtredelsen, men NHRC kan beslutte å undersøke en klage som inngis etter denne fristen, så lenge foreldelsesfristen i henhold til straffe- eller sivilretten ikke er utløpt (artikkel 32 nr. 1 pkt. 4 i NHRC-loven).

([152]) Artikkel 42 ff. i NHRC-loven.

([153]) Artikkel 36 og 37 i NHRC-loven.

([154]) Artikkel 44 i NHRC-loven.

([155]) Artikkel 42 nr. 4 i NHRC-loven.

([156]) Artikkel 48 i NHRC-loven.

([157]) Dersom NHRC unntaksvis for eksempel ikke kan inspisere visse materialer eller fasiliteter fordi de gjelder statshemmeligheter som kan ha en vesentlig innvirkning på statens sikkerhet eller diplomatiske forbindelser, eller dersom inspeksjonen vil utgjøre en alvorlig hindring av en strafferettslig etterforskning eller verserende rettssak (se fotnote 166), og dersom dette hindrer NHRC i å foreta undersøkelsen som kreves for å vurdere om den mottatte klagen er begrunnet, vil NHRC underrette den berørte personen om grunnene til avvisning av klagen, i samsvar med artikkel 39 i NHRC-loven. I dette tilfellet kan enkeltpersonen bestride NHRCs beslutning i henhold til forvaltningsprosessloven.

([158]) Se for eksempel Seouls høyere domstols avgjørelse 2007Nu27259 av 18. april 2008 bekreftet av høyesteretts avgjørelse 2008Du7854 av 9. oktober 2008, Seouls høyesteretts avgjørelse 2017Nu69382 av 2. februar 2018.

([159]) Artikkel 121 og 219 i CPA

([160]) Artikkel 417 sammenholdt med artikkel 414 nr. 2 i CPA. Se også høyesteretts avgjørelse 97Mo66 av 29. september 1997.

Enkeltpersoner kan også oppnå skadeserstatning ved de sørkoreanske domstolene. På grunnlag av loven om statlig erstatning kan enkeltpersoner søke om erstatning for skader som offentlige tjenestemenn forårsaker dersom de utøver sine offisielle arbeidsoppgaver i strid med loven([161]). Et krav i henhold til loven om statlig erstatning kan inngis til et spesialisert «erstatningsråd» eller direkte til de sørkoreanske domstolene([162]). Dersom offeret er en fremmed borger, får loven om statlig erstatning anvendelse så lenge vedkommendes opprinnelsesland også sikrer statlig erstatning for sørkoreanske borgere([163]). I henhold til rettspraksisen er dette vilkåret oppfylt dersom kravene for å anmode om erstatning i det andre landet «ikke i vesentlig grad avviker mellom Sør-Korea og det andre landet» og «generelt sett ikke er strengere enn kravene som er fastsatt av Sør-Korea, uten materielle og vesentlige forskjeller»([164]). Sivilloven regulerer statens erstatningsansvar, og som en følge av dette omfatter statens erstatningsansvar også immaterielle skader (for eksempel problemer av psykisk art)([165]).

Når det gjelder overtredelser av reglene for vern av opplysninger, inneholder PIPA nok et rettsmiddel. I henhold til artikkel 39 i PIPA kan enhver som lider skade som følge av en overtredelse av PIPA eller tap, tyveri, spredning, forfalskning eller endring av eller skade på sine personopplysninger, oppnå skadeserstatning ved domstolene. Det er ikke noe tilsvarende krav om gjensidighet som i loven om statlig erstatning.

I tillegg til skadeserstatning er det adgang til administrativ prøving i forbindelse med forvaltningsorganers tiltak eller unnlatelse av å handle i henhold til forvaltningsprosessloven. Alle enkeltpersoner kan bestride en disposisjon (det vil si utøvelse eller avvisning av å utøve offentlig myndighet i en bestemt sak) eller unnlatelse av å handle (at et forvaltningsorgan over lang tid ikke treffer en bestemt disposisjon tross en rettslig forpliktelse til å gjøre det) som kan føre til tilbakekalling/endring av en ulovlig disposisjon, utstedelse av en avgjørelse om ugyldighet (det vil si om at disposisjonen ikke har rettsvirkning eller ikke eksisterer i rettsordenen) eller om at en unnlatelse av å handle er ulovlig([166]). For å kunne bestride en administrativ disposisjon må den ha direkte innvirkning på borgerrettigheter og -plikter([167]). Dette omfatter tiltak for å samle inn personopplysninger, enten direkte (for eksempel avlytting av kommunikasjon) eller gjennom en anmodning om utlevering (for eksempel til en tjenesteleverandør).

De ovennevnte kravene kan i første omgang bringes inn for administrative klageutvalg nedsatt under visse offentlige myndigheter (for eksempel NIS og NHRC) eller for det sentrale administrative klageutvalget nedsatt under kommisjonen for korrupsjonsbekjempelse og borgerrettigheter([168]). En slik klage til en overordnet forvaltningsmyndighet er en alternativ og mer uformell mulighet til å bestride en offentlig myndighets disposisjon eller unnlatelse av å handle. Et krav kan imidlertid også bringes direkte inn for de sørkoreanske domstolene i henhold til forvaltningsprosessloven.

En anmodning om tilbakekalling/endring av en disposisjon i henhold til forvaltningsprosessloven kan inngis av enhver som har en rettslig interesse av å anmode om tilbakekallingen/endringen, eller av å få sine rettigheter gjenopprettet ved tilbakekallingen/endringen dersom disposisjonen ikke lenger har virkning([169]). På samme måte kan en person som har en rettslig interesse av en slik bekreftelse, anlegge sak for å få fastslått at en disposisjon er ugyldig, mens en sak for å få bekreftet at en unnlatelse av å handle er ulovlig, kan anlegges av enhver som har inngitt en anmodning om en disposisjon og har en rettslig interesse av å få bekreftet at en unnlatelse er ulovlig([170]). I henhold til høyesteretts rettspraksis fortolkes «rettslig interesse» som «en rettslig beskyttet interesse», det vil si en direkte og spesifikk interesse som er beskyttet av lover og forskrifter, og som administrative bestemmelser er basert på (det vil si ikke allmennhetens generelle, indirekte og abstrakte interesser)([171]). Enkeltpersoner har derfor en rettslig interesse ved overtredelse av begrensningene og garantiene for innsamling av deres personopplysninger for formål knyttet til strafferettslig håndheving (i henhold til spesifikke lover eller PIPA). En endelig dom avsagt i henhold til forvaltningsprosessloven er bindene for partene([172]).

([161]) Artikkel 2 nr. 1 i loven om statlig erstatning.

([162]) Artikkel 9 og 12 i loven om statlig erstatning. Ved loven opprettes det distriktsråd (ledet av visestatsadvokaten ved det aktuelle statsadvokatkontoret), et sentralråd (ledet av visejustisministeren) og et spesialråd (ledet av viseforsvarsministeren med ansvar for krav om erstatning for skade forårsaket av militært personell eller sivilt ansatte i militæret). Erstatningskrav behandles i prinsippet av distriktsråd, som under visse omstendigheter skal videresende saker til sentral-/spesialrådet, for eksempel dersom erstatningen overstiger et visst beløp, eller dersom en person anmoder om ny behandling. Alle rådene består av medlemmer utpekt av justisministeren (for eksempel blant offentlige tjenestemenn ved justisdepartementet, domstoler, advokater og personer med ekspertise innen statlig erstatning) og omfattes av særlige regler om interessekonflikter (se artikkel 7 i gjennomføringsdekretet til loven om statlig erstatning).

([163]) Artikkel 7 i loven om statlig erstatning.

([164]) Høyesteretts avgjørelse 2013Da208388 av 11. juni 2015.

([165]) Se artikkel 8 i loven om statlig erstatning og artikkel 751 i sivilloven.

([166]) Artikkel 2 og 4 i forvaltningsprosessloven.

([167]) Høyesteretts avgjørelse 98Du18435 av 22. oktober 1999, høyesteretts avgjørelse 99Du1113 av 8. september 2000 og høyesteretts avgjørelse 2010Du3541 av 27. september 2012.

([168]) Artikkel 6 i loven om klager til overordnet forvaltningsmyndighet og artikkel 18 nr. 1 i forvaltningsprosessloven.

([169]) Artikkel 12 i forvaltningsprosessloven.

([170]) Artikkel 35 og 36 i forvaltningsprosessloven.

([171]) Høyesteretts avgjørelse 2006Du330 av 26. mars 2006.

([172]) Artikkel 30 nr. 1 i forvaltningsprosessloven.

En anmodning om tilbakekalling/endring av en disposisjon og en anmodning om å få bekreftet at en unnlatelse er ulovlig, skal inngis senest 90 dager etter den datoen da personen får kjennskap til disposisjonen/unnlatelsen, og i prinsippet senest et år etter datoen for utstedelsen av disposisjonen, eller datoen for unnlatelsen, med mindre det foreligger berettigede grunner([173]). I henhold til høyesteretts rettspraksis skal begrepet «berettigede grunner» fortolkes i vid forstand og krever at det foretas en vurdering av om det er sosialt akseptabelt å tillate en forsinket klage på bakgrunn av sakens omstendigheter([174]). Dette omfatter for eksempel (men er ikke begrenset til) grunner til forsinkelsen som den berørte parten ikke kan holdes ansvarlig for (det vil si situasjoner som ligger utenfor klagerens kontroll, for eksempel dersom vedkommende ikke er blitt underrettet om innsamlingen av vedkommendes personopplysninger) eller force majeure (for eksempel naturkatastrofe eller krig).

Enkeltpersoner kan også inngi en forfatningsmessig klage til forfatningsdomstolen([175]). På grunnlag av loven om forfatningsdomstolen kan enhver person som får sine grunnleggende forfatningssikrede rettigheter krenket gjennom utøvelse eller manglende utøvelse av offentlig myndighet (unntatt domstolsavgjørelser), inngi en forfatningsmessig klage. Dersom andre rettsmidler er tilgjengelige, skal disse være uttømt først. I henhold til forfatningsdomstolens rettspraksis kan fremmede borgere inngi en forfatningsmessig klage i den grad deres grunnleggende rettigheter er anerkjent i den sørkoreanske forfatningen (se forklaringene i avsnitt 1.1)([176]). Forfatningsmessige klager skal inngis senest 90 dager etter at personen har fått kjennskap til overtredelsen, og senest et år etter at den har funnet sted. En klage skal fremdeles kunne tas opp til behandling dersom det foreligger «berettigede grunner» som fortolket i samsvar med høyesteretts rettspraksis beskrevet ovenfor, ettersom prosedyren i forvaltningsprosessloven får anvendelse på tvister i henhold til loven om forfatningsdomstolen([177]).

Dersom andre rettsmidler må uttømmes først, skal en forfatningsmessig klage inngis senest 30 dager etter den endelige avgjørelsen om et slikt rettsmiddel([178]). Forfatningsdomstolen kan ugyldiggjøre utøvelsen av offentlig myndighet som forårsaket overtredelsen, eller bekrefte at en bestemt unnlatelse av å handle er forfatningsstridig([179]). Da skal den relevante myndigheten treffe tiltak for å etterkomme domstolens avgjørelse.

3. OFFENTLIGE MYNDIGHETERS TILGANG FOR FORMÅL KNYTTET TIL NASJONAL SIKKERHET

3.1. Vedkommende offentlige myndigheter på området nasjonal sikkerhet

Republikken Korea har to spesialiserte etterretningsorganer: NIS og forsvarssikkerhetskommandoen. Ut over dette kan politi og påtalemyndigheter også samle inn personopplysninger for formål knyttet til nasjonal sikkerhet.

NIS er opprettet ved loven om den nasjonale etterretningstjenesten (National Intelligence Service Act, heretter kalt «NIS-loven») og er direkte underlagt presidentens myndighet og tilsyn([180]). NIS samler inn, kompilerer og sprer informasjon om andre land (og Nord-Korea)([181]), etterretning knyttet til kontraspionasje (herunder militær- og industrispionasje), terrorisme og internasjonale kriminelle syndikaters aktiviteter, etterretning om visse typer straffbare handlinger rettet mot offentlig og nasjonal sikkerhet (for eksempel innenlandsk opprør, aggresjon utenfra) og etterretning knyttet til oppgavene med å sikre cybersikkerheten og forebygge eller bekjempe cyberangrep og -trusler([182]). I NIS-loven, som NIS ble opprettet ved, fastsettes etterretningstjenestens oppgaver og de generelle prinsippene som danner grunnlaget for alle dens aktiviteter. NIS skal som et generelt prinsipp være politisk nøytralt og beskytte enkeltpersoners rettigheter og friheter([183]). Direktøren for NIS har som oppgave å utarbeide generelle retningslinjer for prinsippene, omfanget og prosedyrene for NIS' oppgaver i forbindelse med innsamling og bruk av opplysninger, og skal rapportere disse til nasjonalforsamlingen([184]). Nasjonalforsamlingen kan (gjennom sitt etterretningsutvalg) kreve at retningslinjene korrigeres eller utfylles dersom den mener at de er ulovlige eller urettmessige. Mer generelt kan direktøren for og de ansatte i NIS, når de utfører sine oppgaver, ikke tvinge en institusjon, organisasjon eller enkeltperson til å gjøre noe de ikke er forpliktet til, eller hindre en person i å utøve sine rettigheter, ved å misbruke sin offentlige myndighet([185]). Dessuten skal enhver form for sensur av post, avlytting av telekommunikasjon, innsamling av

([173]) Artikkel 20 i forvaltningsprosessloven. Denne fristen gjelder også for et krav om å få bekreftet at en unnlatelse er ulovlig, se artikkel 38 nr. 2 i forvaltningsprosessloven.
([174]) Høyesteretts avgjørelse 90Nu6521 av 28. juni 1991.
([175]) Artikkel 68 nr. 1 i loven om forfatningsdomstolen.
([176]) Forfatningsdomstolens avgjørelse 99HeonMa194 av 29. november 2001.
([177]) Artikkel 40 i loven om forfatningsdomstolen.
([178]) Artikkel 69 i loven om forfatningsdomstolen.
([179]) Artikkel 75 nr. 3 i loven om forfatningsdomstolen.
([180]) Artikkel 2 og artikkel 4 nr. 2 i NIS-loven.
([181]) Dette begrepet omfatter ikke opplysninger om enkeltpersoner, men generell informasjon om andre land (tendenser, utvikling) og om aktiviteter som utføres av statlige aktører i tredjeland.
([182]) Artikkel 3 nr. 1 i NIS-loven.
([183]) Artikkel 3 nr. 1, artikkel 6 nr. 2 og artikkel 11 og 21. Se også reglene for interessekonflikter, særlig artikkel 10 og 12.
([184]) Artikkel 4 nr. 2 i NIS-loven.
([185]) Artikkel 13 i NIS-loven.

lokaliseringsopplysninger, innsamling av kommunikasjonsbekreftelsesdata eller registrering av eller lytting til privat kommunikasjon som utføres av NIS, være i samsvar med CPPA, lokaliseringsopplysningsloven eller CPA([186]). Ethvert misbruk av myndighet eller innsamling av opplysninger i strid med disse lovene omfattes av strafferettslige sanksjoner([187]).

Forsvarssikkerhetskommandoen er et militært etterretningsorgan opprettet under forsvarsdepartementet. Den har ansvar for militære sikkerhetsspørsmål, militære strafferettslige etterforskninger (som omfattes av loven om militærdomstolen) og militær etterretning. Forsvarssikkerhetskommandoen overvåker generelt sett ikke sivile, med mindre dette er nødvendig for å ivareta dens militære funksjoner. Personer som kan etterforskes, er militært personell, sivilt ansatte i militæret, personer under militær opplæring, reservister, rekrutter og krigsfanger([188]). Når forsvarssikkerhetskommandoen samler inn kommunikasjonsopplysninger for formål knyttet til nasjonal sikkerhet, er den underlagt begrensningene og garantiene fastsatt i CPPA og gjennomføringsdekretet til den.

3.2. **Rettslig grunnlag og begrensninger**

CPPA, loven om terrorbekjempelse og beskyttelse av borgere og den offentlige sikkerhet (heretter kalt «antiterrorloven») og TBA utgjør det rettslige grunnlaget for innsamling av personopplysninger for formål knyttet til nasjonal sikkerhet og fastsetter gjeldende begrensninger og garantier([189]). Disse begrensningene og garantiene, som beskrives i de neste avsnittene, sikrer at innsamlingen og behandlingen av opplysninger er begrenset til det som er strengt nødvendig for å nå et berettiget mål. Dette utelukker masseinnsamling og vilkårlig innsamling av personopplysninger for formål knyttet til nasjonal sikkerhet.

3.2.1. *Innsamling av kommunikasjonsopplysninger*

3.2.1.1. Etterretningsorganers innsamling av kommunikasjonsopplysninger

3.2.1.1.1. Rettslig grunnlag

CPPA gir etterretningsorganer myndighet til å samle inn kommunikasjonsopplysninger og krever at kommunikasjonsleverandører skal samarbeide ved anmodninger fra disse organene([190]). Som beskrevet i avsnitt 2.2.2.1 skilles det i CPPA mellom innsamling av kommunikasjonsinnhold (det vil si «kommunikasjonsbegrensende tiltak», for eksempel «avlytting» eller «sensor»([191])) og innsamling av «kommunikasjonsbekreftelsesdata»([192]).

Terskelen for innsamling av disse to typene opplysninger varierer, men de gjeldende prosedyrene og garantiene er i stor grad identiske([193]). Innsamling av kommunikasjonsbekreftelsesdata (eller metadata) kan skje for å forebygge trusler mot den nasjonale sikkerheten([194]). Det er en høyere terskel for å gjennomføre kommunikasjonsbegrensende tiltak (det vil si innsamling av kommunikasjonsinnhold), som bare kan treffes dersom det forventes at den nasjonale sikkerheten vil bli utsatt for alvorlig fare, og innsamling av etterretning er nødvendig for å avverge en slik fare (det vil si dersom det foreligger en alvorlig risiko for den nasjonale sikkerheten, og innsamlingen er nødvendig for å avverge denne)([195]). Det skal dessuten bare gis tilgang til kommunikasjonsinnhold som en siste utvei for å sikre den nasjonale sikkerheten, og det skal gjøres en innsats for å minimere krenkingen av personvernet i forbindelse med kommunikasjon([196]). Også når den relevante godkjenningen/tillatelsen er innhentet, skal slike tiltak opphøre umiddelbart når de ikke lenger er nødvendige, noe som sikrer at krenkingen av den enkeltes rett til kommunikasjonshemmelighet begrenses til et minimum([197]).

3.2.1.1.2. Begrensninger og garantier for innsamling av kommunikasjonsopplysninger som omfatter minst én sørkoreansk borger

([186]) Artikkel 14 i NIS-loven.
([187]) Artikkel 22 og 23 i NIS-loven.
([188]) Artikkel 1 i loven om militærdomstolen.
([189]) Ved etterforskning av straffbare handlinger knyttet til den nasjonale sikkerheten er politiet og NIS underlagt CPA, mens forsvarssikkerhetskommandoen er underlagt loven om militærdomstolen.
([190]) Artikkel 15-2 i CPPA.
([191]) Artikkel 2 nr. 6 og 7 i CPPA.
([192]) Artikkel 2 nr. 11 i CPPA.
([193]) Se også artikkel 13-4 nr. 2 i CPPA og artikkel 37 nr. 4 i gjennomføringsdekretet til CPPA, der det er fastsatt at prosedyrene som gjelder for innsamling av kommunikasjonsinnhold, gjelder tilsvarende med nødvendige endringer for innsamling av kommunikasjonsbekreftelsesdata.
([194]) Artikkel 13-4 i CPPA.
([195]) Artikkel 7 nr. 1 i CPPA.
([196]) Artikkel 3 nr. 2 i CPPA.
([197]) Artikkel 2 i gjennomføringsdekretet til CPPA.

Innsamling av kommunikasjonsopplysninger (både innhold og metadata) der en av eller begge parter i kommunikasjonen er sørkoreanske borgere, kan bare skje med tillatelse fra en overdommer ved en høyere domstol([198]). Anmodningen fra etterretningsorganet skal inngis skriftlig til en statsadvokat eller en høyere påtalemyndighet([199]). I den skal det opplyses om grunnene til innsamlingen (det vil si at det forventes at den nasjonale sikkerheten vil bli utsatt for alvorlig fare, eller at innsamlingen er nødvendige for å forebygge trusler mot den nasjonale sikkerheten), og den skal inneholde materiale som underbygger disse grunnene og viser at det foreligger en *prima facie*-sak, samt nærmere opplysninger om anmodningen (det vil si formålene, den eller de berørte personene, omfang, faktisk innsamlingsperiode og hvordan og hvor innsamlingen vil finne sted)([200]). Statsadvokaten / den høyere påtalemyndigheten skal deretter anmode om tillatelse fra en overdommer ved en høyere domstol([201]). Overdommeren kan bare gi skriftlig tillatelse dersom han/hun mener at søknaden er berettiget, og vil avvise anmodningen dersom han/hun anser den for å være ubegrunnet([202]). I kjennelsen angis type, formål, mål, omfang og faktisk innsamlingsperiode samt hvor og hvordan den skal finne sted([203]).

Det gjelder særlige regler dersom tiltaket gjelder etterforskning av en sammensvergelse som truer den nasjonale sikkerheten, og det foreligger en nødssituasjon som gjør det umulig å gjennomføre de ovennevnte prosedyrene([204]). Dersom disse vilkårene er oppfylt, kan etterretningsorganer gjennomføre overvåkingstiltak uten forutgående domstolsgodkjenning([205]). Umiddelbart etter gjennomføringen av hastetiltakene skal etterretningsorganet anmode om tillatelse fra domstolen. Dersom det ikke er oppnådd tillatelse senest 36 timer etter at tiltakene er truffet, skal de opphøre umiddelbart([206]). Innsamling av opplysninger i nødssituasjoner skal alltid skje i samsvar med en «erklæring om sensur/avlytting i nødssituasjoner», og etterretningsorganet som foretar innsamlingen, skal føre et register over eventuelle hastetiltak([207]).

Dersom overvåkingen avsluttes i løpet av kort tid og uten rettskjennelse, skal lederen for vedkommende høyere påtalemyndighet sende en melding om hastetiltak utarbeidet av etterretningsorganet til lederen for vedkommende domstol, som skal inneha registeret over hastetiltak([208]). Dette gjør det mulig for domstolen å undersøke om innsamlingen er lovlig.

3.2.1.1.3. Begrensninger og garantier for innsamling av kommunikasjonsopplysninger som bare omfatter fremmede borgere

For å samle inn opplysninger om kommunikasjon mellom bare ikke-sørkoreanske borgere skal etterretningsorganene innhente skriftlig forhåndstillatelse fra presidenten([209]). Slik kommunikasjon kan bare samles inn for formål knyttet til nasjonal sikkerhet dersom kommunikasjonen inngår i en av flere angitte kategorier, det vil si kommunikasjon mellom statstjenestemenn eller andre enkeltpersoner fra land som er fiendtlig innstilte mot Republikken Korea, utenlandske organer, grupper eller statsborgere som mistenkes for å delta i aktiviteter som kan skade Republikken Korea([210]), eller medlemmer av grupper som opererer på Koreahalvøya, men uten reelt å være underlagt Republikken Koreas suverenitet, og deres paraplygrupper basert i andre land([211]). Dersom den ene parten i kommunikasjonen er en sørkoreansk borger og den andre en fremmed borger, kreves det imidlertid domstolsgodkjenning i samsvar med framgangsmåten beskrevet i avsnitt 3.2.1.1.2.

Lederen for et etterretningsorgan skal framlegge en plan for tiltakene det planlegges å treffe, for direktøren for NIS([212]). Direktøren for NIS skal vurdere om planen er hensiktsmessig og, dersom det er tilfellet, framlegge den for presidenten for godkjenning([213]). Planen skal inneholde den samme informasjonen som den som kreves for en søknad om domstolstillatelse til å samle inn informasjon fra sørkoreanske borgere (som beskrevet over)([214]). Den skal særlig inneholde informasjon om grunnene til innsamlingen (det vil si at det forventes at den nasjonale sikkerheten vil bli utsatt for alvorlig fare, eller at

([198]) Artikkel 7 nr. 1 pkt. 1 i CPPA. Vedkommende domstol er den høyere domstolen som har kompetanse på det stedet der den ene eller begge de overvåkede partene har sitt bosted eller sete.
([199]) Artikkel 7 nr. 3 i gjennomføringsdekretet til CPPA.
([200]) Artikkel 7 nr. 3 og artikkel 6 nr. 4 i CPPA.
([201]) Artikkel 7 nr. 4 i gjennomføringsdekretet til CPPA. I anmodningen til domstolen angis de viktigste grunnene til mistanke og, dersom det bes om flere tillatelser samtidig, begrunnelsen for dette (se artikkel 4 i gjennomføringsdekretet til CPPA).
([202]) Artikkel 7 nr. 3, artikkel 6 nr. 5 og artikkel 6 nr. 9 i CPPA.
([203]) Artikkel 7 nr. 3 og artikkel 6 nr. 6 i CPPA.
([204]) Artikkel 8 i CPPA.
([205]) Artikkel 8 nr. 1 i CPPA.
([206]) Artikkel 8 nr. 2 i CPPA.
([207]) Artikkel 8 nr. 4 i CPPA. Se avsnitt 2.2.2.2. over for hastetiltak i forbindelse med rettshåndheving.
([208]) Artikkel 8 nr. 5 og 7 i CPPA. I denne meldingen angis formålet, målet, omfanget, varigheten, gjennomføringsstedet og overvåkingsmetoden samt grunnene til at det ikke ble inngitt en begjæring før tiltakene ble truffet (artikkel 8 nr. 6 i CPPA).
([209]) Artikkel 7 nr. 1 pkt. 2 i CPPA.
([210]) Dette dreier seg om aktiviteter som truer nasjonens eksistens og sikkerhet, den demokratiske orden eller folkets overlevelse og frihet.
([211]) Dersom den ene parten er en person som beskrevet i artikkel 7 nr. 1 pkt. 2 i CPPA og den andre er ukjent eller ikke kan identifiseres, får prosedyren beskrevet i artikkel 7 nr. 1 pkt. 2 anvendelse.
([212]) Artikkel 8 nr. 1 i gjennomføringsdekretet til CPPA. Direktøren for NIS utnevnes av presidenten med parlamentets godkjenning (artikkel 7 i NIS-loven).
([213]) Artikkel 8 nr. 2 i gjennomføringsdekretet til CPPA.
([214]) Artikkel 8 nr. 3 i gjennomføringsdekretet til CPPA sammenholdt med artikkel 6 nr. 4 i CPPA.

innsamlingen er nødvendige for å forebygge trusler mot den nasjonale sikkerheten), hovedgrunnene til mistanke og materiale som underbygger disse grunnene og viser at det foreligger en *prima facie*-sak, samt nærmere opplysninger om anmodningen (det vil si formålene, den eller de berørte personene, omfang, faktisk innsamlingsperiode og hvordan og hvor innsamlingen vil finne sted). Dersom det anmodes om flere tillatelser samtidig, angis formål og begrunnelse([215]).

I nødssituasjoner([216]) skal det innhentes forhåndsgodkjenning fra ministeren som det relevante etterretningsorganet er underlagt. I dette tilfellet skal etterretningsorganet imidlertid anmode om presidentens godkjenning umiddelbart etter at hastetiltakene er truffet. Dersom et etterretningsorgan ikke oppnår godkjenning senest 36 timer etter at anmodningen er inngitt, skal innsamlingen opphøre umiddelbart([217]). I slike tilfeller vil de innsamlede opplysningene alltid bli tilintetgjort.

3.2.1.1.4. Generelle begrensninger og garantier

Når etterretningsorganer anmoder private enheter om å samarbeide, skal de gi dem rettskjennelsen / tillatelsen fra presidenten eller en kopi av forsiden på en erklæring om sensur i nødssituasjoner, som den aktuelle enheten skal oppbevare([218]). Enheter som anmodes om å utlevere opplysninger til etterretningsorganer på grunnlag av CPPA, kan nekte å gjøre det dersom godkjenningen eller erklæringen om sensur i nødssituasjoner inneholder en feil identifikator (for eksempel et telefonnummer som tilhører en annen person enn den identifiserte personen). Passord som brukes i forbindelse med kommunikasjon, skal ikke under noen omstendigheter utleveres([219]).

Etterretningsorganer kan overføre gjennomføringen av kommunikasjonsbegrensende tiltak eller innsamling av kommunikasjonsbekreftelsesdata til et postkontor eller en leverandør av telekommunikasjonstjenester (som definert i loven om telekommunikasjonsvirksomhet)([220]). Både det relevante etterretningsorganet og leverandøren som mottar en anmodning om samarbeid, skal føre registre over formålet med anmodningen om tiltak, datoen for gjennomføringen eller samarbeidet og hva tiltakene er rettet mot (for eksempel post, telefon, e-post) i tre år([221]). Leverandører av telekommunikasjonstjenester som videreformidler kommunikasjonsbekreftelsesdata, skal oppbevare informasjon om innsamlingshyppigheten i sju år og rapportere til ministeren for vitenskap og IKT to ganger i året([222]).

Etterretningsorganer skal rapportere om opplysningene de har samlet inn, og om utfallet av overvåkingen, til direktøren for NIS([223]). Når det gjelder innsamling av kommunikasjonsbekreftelsesdata, skal det føres registre over at det er inngitt en anmodning om slike data, og over selve den skriftlige anmodningen og institusjonen som baserer seg på den([224]).

Innsamlingen av både kommunikasjonsinnhold og kommunikasjonsbekreftelsesdata kan pågå i høyst fire måneder og skal umiddelbart opphøre dersom målet som forfølges, nås tidligere([225]). Dersom vilkårene for tillatelsen fortsatt er oppfylt, kan fristen forlenges med opptil fire måneder med domstolens tillatelse eller presidentens godkjenning. Søknaden om å få godkjent en forlengelse av overvåkingstiltakene skal inngis skriftlig med en angivelse av grunnene til at det bes om forlengelse, og det skal vedlegges dokumentasjon([226]).

Avhengig av det rettslige grunnlaget for innsamlingen underrettes enkeltpersoner vanligvis når deres kommunikasjon samles inn. Uansett om de innsamlede opplysningene gjelder kommunikasjonsinnhold eller kommunikasjonsbekreftelsesdata, og uansett om opplysningene ble innhentet etter den vanlige prosedyren eller i en nødssituasjon, skal lederen for etterretningsorganet underrette den berørte personen om overvåkingstiltaket senest 30 dager etter at overvåkingen opphørte([227]). I underretningen

([215]) Artikkel 8 nr. 3 og artikkel 4 i gjennomføringsdekretet til CPPA.
([216]) Det vil si når tiltakene gjelder en sammensvergelse som truer den nasjonale sikkerheten, og det ikke er tilstrekkelig tid til å innhente godkjenning fra presidenten og manglende hastetiltak kan skade den nasjonale sikkerheten (artikkel 8 nr. 8 i CPPA).
([217]) Artikkel 8 nr. 9 i CPPA.
([218]) Artikkel 9 nr. 2 i CPPA og artikkel 12 i gjennomføringsdekretet til CPPA.
([219]) Artikkel 9 nr. 4 i CPPA.
([220]) Artikkel 13 i gjennomføringsdekretet til CPPA.
([221]) Artikkel 9 nr. 3 i CPPA og artikkel 17 nr. 2 i gjennomføringsdekretet til CPPA. Denne perioden får ikke anvendelse på kommunikasjonsbekreftelsesdata (se artikkel 39 i gjennomføringsdekretet til CPPA).
([222]) Artikkel 13 nr. 7 i CPPA og artikkel 39 i gjennomføringsdekretet til CPPA.
([223]) Artikkel 18 nr. 3 i gjennomføringsdekretet til CPPA.
([224]) Artikkel 13 nr. 5 og artikkel 13-4 nr. 3 i CPPA.
([225]) Artikkel 7 nr. 2 i CPPA.
([226]) Artikkel 7 nr. 2 i CPPA og artikkel 5 i gjennomføringsdekretet til CPPA.
([227]) Artikkel 9-2 nr. 3 i CPPA. I samsvar med artikkel 13-4 i CPPA får dette anvendelse på innsamling av både kommunikasjonsinnhold og kommunikasjonsbekreftelsesdata.

skal følgende angis: 1) At opplysninger er samlet inn, 2) hvem som har samlet dem inn, og 3) gjennomføringsperioden. Dersom det er sannsynlig at underretningen vil bringe den nasjonale sikkerheten i fare eller skade menneskers liv og fysiske sikkerhet, kan underretningen imidlertid utsettes([228]). Underretningen skal gis senest 30 dager etter at grunnene til utsettelsen ikke lenger foreligger([229]).

Dette kravet til underretning gjelder imidlertid bare for innsamling av opplysninger der minst én av partene er sørkoreansk statsborger. Ikke-sørkoreanske borgere vil derfor bare bli underrettet når deres kommunikasjon med sørkoreanske statsborgere samles inn. Det er derfor ingen krav til underretning når det samles inn kommunikasjon utelukkende mellom ikke-sørkoreanske borgere.

Innholdet i all kommunikasjon og kommunikasjonsbekreftelsesdata som samles inn gjennom overvåking på grunnlag av CPPA, kan bare brukes 1) til etterforskning, rettsforfølgning eller forebygging av visse straffbare forhold, 2) i disiplinærsaker, 3) i retterganger der en part i kommunikasjonen påberoper seg dette i et krav om skadeserstatning, eller 4) på grunnlag av annen lovgivning([230]).

3.2.1.2. Politiets/påtalemyndighetens innsamling av kommunikasjonsopplysninger for formål knyttet til nasjonal sikkerhet.

Politiet/påtalemyndigheten kan samle inn kommunikasjonsopplysninger (både kommunikasjonsinnhold og kommunikasjonsbekreftelsesdata) for formål knyttet til nasjonal sikkerhet på de samme vilkårene som de som er beskrevet i avsnitt 3.2.1.1. I nødssituasjoner([231]) brukes framgangsmåten beskrevet tidligere for innsamling av kommunikasjonsinnhold for rettshåndhevende formål i nødssituasjoner (det vil si artikkel 8 i CPPA).

3.2.2. *Innsamling av opplysninger om terrormistenkte*

3.2.2.1. Rettslig grunnlag

Antiterrorloven gir direktøren for NIS myndighet til å samle inn opplysninger om terrormistenkte([232]). En «terrormistenkt» defineres som et medlem av en terrorgruppe([233]), en person som har drevet propaganda for en terrorgruppe (ved å fremme og spre en terrorgruppes ideer og taktikk), samlet inn penger til eller bidratt til finansiering av terrorisme([234]) eller deltatt i andre aktiviteter, for eksempel forberedelse av, sammensvergelse til, spredning av propaganda for eller oppmuntring til terrorisme, eller en person der det er begrunnet mistanke om at vedkommende har deltatt i slike aktiviteter([235]). Som en generell regel skal alle offentlige tjenestemenn som håndhever antiterrorloven, respektere de grunnleggende rettighetene som er nedfelt i den sørkoreanske forfatningen([236]).

I antiterrorloven er det ikke fastsatt spesifikk myndighet eller spesifikke begrensninger og garantier for innsamling av opplysninger om terrormistenkte, det vises i stedet til prosedyrene i andre lover. For det første kan direktøren for NIS på grunnlag av antiterrorloven samle inn 1) opplysninger om innreise til og utreise fra Republikken Korea, 2) om finansielle transaksjoner og 3) om kommunikasjon. Avhengig av hvilken type opplysninger det er behov for, er de relevante prosessuelle kravene fastsatt i henholdsvis immigrasjonsloven, tolloven, ARUSFTI eller CPPA([237]). Når det gjelder innsamling av opplysninger om innreise til og utreise fra Republikken Korea, viser antiterrorloven til prosedyrene fastsatt i immigrasjonsloven

([228]) Artikkel 9-2 nr. 4 i CPPA.

([229]) Artikkel 13-4 nr. 2 og 9-2 nr. 6 i CPPA.

([230]) Artikkel 5 nr.1–2, artikkel 12 og artikkel 13-5 i CPPA.

([231]) Det vil si dersom tiltaket gjelder en sammensvergelseshandling som truer den nasjonale sikkerheten, og det foreligger en nødssituasjon som gjør det umulig å følge den vanlige godkjenningsprosedyren (artikkel 8 nr. 1 i CPPA).

([232]) Artikkel 9 i antiterrorloven.

([233]) «Terrorgruppe» defineres som en gruppe terrorister som er oppført på FNs liste (artikkel 2 nr. 2 i antiterrorloven).

([234]) «Terrorisme» defineres i artikkel 2 nr. 1 i antiterrorloven som handlinger som utføres for å hindre statens, en lokal myndighets eller en utenlandsk regjerings (herunder lokale myndigheter og internasjonale organisasjoner) myndighetsutøvelse, å tvinge dem til å handle uten at de er rettslig forpliktet til det, eller å true allmennheten. Dette omfatter a) drap på en person eller å utsette en person for livsfare ved å forårsake kroppsskade eller ved anholdelse, innesperring, kidnapping eller gisseltaking av en person, b) visse handlinger rettet mot et luftfartøy (for eksempel å styrte, kapre eller skade et luftfartøy under en flygning), c) visse typer handlinger rettet mot et skip (for eksempel å ta beslag i et skip eller en marin struktur i drift, ødelegge et skip eller en marin struktur i drift eller skade dette i et omfang som bringer sikkerheten i fare, herunder skade på lasten på skipet eller den marine strukturen i drift), d) å plassere, detonere eller på annen måte bruke et biokjemisk eller eksplosivt våpen eller brannvåpen eller utstyr med det formål å forårsake død, alvorlig skade eller alvorlig materiell skade eller som har slik innvirkning på visse typer kjøretøyer eller anlegg (for eksempel tog, trikker, motorvogner, offentlige parker og stadioner, elektrisitets- og gassforsyningsanlegg, telekommunikasjonsanlegg osv.), e) visse typer handlinger i forbindelse med kjernefysisk materiale, radioaktivt materiale eller kjernekraftanlegg (for eksempel skade på menneskers liv, legeme eller eiendom eller forstyrrelse av den offentlige sikkerhet ved å ødelegge en kjernereaktor eller forsettlig feilhåndtering av radioaktivt materiale osv.).

([235]) Artikkel 2 nr. 3 i antiterrorloven.

([236]) Artikkel 3 nr. 3 i antiterrorloven.

([237]) Artikkel 9 nr. 1 i antiterrorloven.

og tolloven. Disse loven inneholder på det nåværende tidspunkt imidlertid ingen bestemmelser om slik myndighet. Når det gjelder innsamling av kommunikasjonsopplysninger og opplysninger om finansielle transaksjoner, viser antiterrorloven til begrensningene og garantiene i CPPA (som beskrives nærmere nedenfor) og ARUSFTI (som, som forklart i avsnitt 2.1, ikke er relevant for vurderingen i forbindelse med beslutningen om tilstrekkelig beskyttelsesnivå).

I artikkel 9 nr. 3 i antiterrorloven presiseres det dessuten at direktøren for NIS kan anmode om personopplysninger eller lokaliseringsopplysninger om en terrormistenkt fra en behandlingsansvarlig([238]) eller en leverandør av lokaliseringsopplysninger([239]). Denne muligheten er begrenset til anmodninger om frivillig utlevering, som behandlingsansvarlige og leverandører av lokaliseringsopplysninger ikke plikter å svare på, og som de i alle tilfeller bare kan svare på i samsvar med PIPA og lokaliseringsopplysningsloven (se avsnitt 3.2.2.2 nedenfor).

3.2.2.2. Begrensninger og garantier for frivillig utlevering i henhold til PIPA og lokaliseringsopplysningsloven

Anmodninger om frivillig samarbeid i henhold til antiterrorloven skal begrenses til opplysninger om terrormistenkte (se avsnitt 3.2.2.1 over). En slik anmodning fra NIS skal være i samsvar med prinsippene om lovlighet, nødvendighet og forholdsmessighet som følger av den sørkoreanske forfatningen (artikkel 12 nr. 1 og artikkel 37 nr. 2)([240]), og kravene til innsamling av personopplysninger i PIPA (artikkel 3 nr. 1 i PIPA, se avsnitt 1.2 over). Det presiseres videre i NIS-loven at NIS ikke kan tvinge en institusjon, organisasjon eller enkeltperson til å gjøre noe de ikke er forpliktet til, eller hindre en person i å utøve sine rettigheter, ved å misbruke sin offentlige myndighet([241]). En overtredelse av dette forbudet kan føre til strafferettslige sanksjoner([242]).

Behandlingsansvarlige og leverandører av lokaliseringsopplysninger som mottar anmodninger fra NIS på grunnlag av antiterrorloven, plikter ikke å etterkomme dem. De kan etterkomme dem frivillig, men bare i samsvar med PIPA og lokaliseringsopplysningsloven. Når det gjelder samsvar med PIPA, skal en behandlingsansvarlig særlig ta hensyn til den registrertes interesser og må ikke utlevere opplysningene dersom det er sannsynlig at det vil krenke vedkommendes eller en tredjeparts interesser urettmessig([243]). Den registrerte skal i henhold til melding 2021-1 om utfyllende regler for fortolkning og anvendelse av loven om vern av personopplysninger i tillegg underrettes om utleveringen. I unntakstilfeller kan en slik underretning utsettes, særlig dersom og så lenge underretningen vil kunne bringe en pågående strafferettslig etterforskning i fare eller det er sannsynlig at det vil skade en annen persons liv eller legeme, dersom disse rettighetene eller interessene klart går foran den registrertes rettigheter ([244]).

3.2.2.3. Begrensninger og garantier i henhold til CPPA

På grunnlag av antiterrorloven kan etterretningsorganer bare samle inn kommunikasjonsopplysninger (både kommunikasjonsinnhold og kommunikasjonsbekreftelsesdata) dersom det er nødvendig i forbindelse med terrorbekjempelsesaktiviteter, det vil si aktiviteter knyttet til forebygging av og mottiltak mot terrorisme. Prosedyrene i CPPA som er beskrevet i avsnitt 3.2.1, får anvendelse på innsamling av kommunikasjonsopplysninger med henblikk på bekjempelse av terrorisme.

3.2.3. *Teleoperatørers frivillige utlevering av opplysninger*

På grunnlag av TBA kan teleoperatører etterkomme en anmodning om utlevering av «kommunikasjonsopplysninger» fra et etterretningsorgan som har til hensikt å samle inn opplysningene for å avverge en trussel mot den nasjonale sikkerheten([245]). En slik anmodning skal være i samsvar med prinsippene om lovlighet, nødvendighet og forholdsmessighet som følger av den sørkoreanske forfatningen (artikkel 12 nr. 1 og artikkel 37 nr. 2)([246]), og kravene til innsamling av personopplysninger i PIPA (artikkel 3 nr. 1 i PIPA, se avsnitt 1.2 over). Dessuten gjelder de samme begrensningene og garantiene som for frivillig utlevering for rettshåndhevende formål (se avsnitt 2.2.3)([247]).

([238]) Som definert i artikkel 2 i PIPA, det vil si en offentlig institusjon, juridisk person, organisasjon, enkeltperson osv. som behandler personopplysninger direkte eller indirekte for å administrere personopplysningsfiler for offisielle eller forretningsmessige formål.

([239]) Som definert i artikkel 5 i loven om vern, bruk osv. av lokaliseringsopplysninger (heretter kalt «lokaliseringsopplysningsloven»), det vil si enhver som har fått tillatelse fra Republikken Koreas kommunikasjonskommisjon til å arbeide med lokaliseringsopplysninger.

([240]) Se også artikkel 3 nr. 2 og 3 i antiterrorloven.

([241]) Artikkel 11 nr. 1 i NIS-loven.

([242]) Artikkel 19 i NIS-loven.

([243]) Artikkel 18 nr. 2 i PIPA.

([244]) Melding 2021-1 fra PIPC om utfyllende regler for fortolkning og anvendelse av loven om vern av personopplysninger, avsnitt III nr. 2 punkt iii).

([245]) Artikkel 83 nr. 3 i TBA.

([246]) Se også artikkel 3 nr. 2 og 3 i antiterrorloven.

([247]) Anmodningen skal særlig være skriftlig og inneholde en begrunnelse for anmodningen samt lenken til den relevante brukeren og omfanget av de ønskede opplysningene, og teleoperatøren skal føre registre og rapportere til ministeren for vitenskap og IKT to ganger i året.

En teleoperatør plikter ikke å etterkomme anmodningen, men kan gjøre dette frivillig og da bare i samsvar med PIPA. I denne forbindelse gjelder de samme forpliktelsene, herunder med hensyn til underretning av den berørte personen, for teleoperatører som når de mottar anmodninger fra strafferettshåndhevende myndigheter, som forklart nærmere i avsnitt 2.2.3.

3.3. **Tilsyn**

Forskjellige organer fører tilsyn med de sørkoreanske etterretningsorganenes aktiviteter. Tilsynet med forsvars-sikkerhetskommandoen utføres av forsvarsdepartementet i henhold til departementets direktiv om gjennomføring av internrevisjon. Tilsynet med NIS utføres av den utøvende makt, nasjonalforsamlingen og andre uavhengige organer som forklart nærmere nedenfor.

3.3.1. *Den ansvarlige for vern av menneskerettigheter*

I henhold til antiterrorloven skal antiterrorkommisjonen og den ansvarlige for vern av menneskerettigheter (Human Rights Protection Officer, heretter kalt «HRPO») føre tilsyn med etterretningsorganers innsamling av opplysninger om terrormistenkte([248]).

Antiterrorkommisjonen utarbeider blant annet strategier for terrorbekjempelsesaktiviteter og fører tilsyn med gjennomføringen av terrorbekjempelsestiltak samt forskjellige vedkommende myndigheters aktiviteter på området terrorbekjempelse([249]). Kommisjonen ledes av statsministeren og består av flere ministere og ledere for statlige organer, herunder utenriksministeren, justisministeren, forsvarsministeren, innenriks- og sikkerhetsministeren, direktøren for NIS, generalkommissæren for den nasjonale politimyndigheten og lederen for kommisjonen for finansielle tjenester([250]). Når det gjennomføres etterforskninger med henblikk på terrorbekjempelse og sporing av terrormistenkte for å samle inn opplysninger eller materiale som kreves for å bekjempe terrorisme, skal direktøren for NIS rapportere til lederen for antiterrorkommisjonen (det vil si statsministeren)([251]).

HRPO er opprettet ved antiterrorloven for å verne enkeltpersoners grunnleggende rettigheter mot overtredelser forårsaket av terrorbekjempelsesaktiviteter([252]). HRPO utnevnes av lederen for antiterrorkommisjonen blant personer som oppfyller kvalifikasjonene angitt i gjennomføringsdekretet til antiterrorloven (det vil si enhver person med kvalifikasjoner som advokat og med minst ti års arbeidserfaring eller med ekspertkunnskap på området menneskerettigheter og som arbeider eller har arbeidet (minst) som assisterende professor i minst ti år, eller som har innehatt en stilling som høyere offentlig tjenestemann i statlige organer eller ved lokale myndigheter, eller med minst ti års arbeidserfaring på området menneskerettigheter, for eksempel i en ikke-statlig organisasjon)([253]). HRPO utnevnes for to år (med mulighet for fornyet mandatperiode) og kan bare avsettes av spesifikke og begrensede grunner og dersom det er berettiget, for eksempel dersom det er reist tiltale i en straffesak knyttet til vedkommendes oppgaver, dersom det er utlevert konfidensielle opplysninger eller på grunn langvarig svekket psykisk eller fysisk funksjonsevne([254]).

Når det gjelder myndighet, kan HRPO utstede anbefalinger for å forbedre måten organer som er involvert i terrorbe-kjempelsesaktiviteter, beskytter menneskerettighetene på, og behandle sivile klager (se avsnitt 3.4.3)([255]). Dersom det med rimelighet kan fastslås at det har skjedd en krenking av menneskerettighetene i forbindelse med offentlig tjenesteutøvelse, kan HRPO utstede en anbefaling til lederen for det ansvarlige organet om å korrigere dette([256]). Det ansvarlige organet skal deretter underrette HRPO om tiltakene som er truffet for å gjennomføre en slik anbefaling([257]). Dersom et organ ikke gjennomfører en anbefaling fra HRPO, sendes saken videre til kommisjonen, herunder lederen, statsministeren. Hittil har det ikke vært tilfeller der HRPOs anbefalinger ikke er blitt gjennomført.

3.3.2. *Nasjonalforsamlingen*

Som beskrevet i avsnitt 2.3.2 kan nasjonalforsamlingen undersøke og granske offentlige myndigheter og i den forbindelse anmode om utlevering av dokumenter og pålegge vitner å møte. Når det gjelder saker som hører inn under NIS' myndighet, utføres dette parlamentariske tilsynet av nasjonalforsamlingens etterretningsutvalg([258]). Direktøren for NIS, som fører tilsyn

([248]) Artikkel 7 i antiterrorloven.
([249]) Artikkel 5 nr. 3 i antiterrorloven.
([250]) Artikkel 3 nr. 1 i gjennomføringsdekretet til antiterrorloven.
([251]) Artikkel 9 nr. 4 i antiterrorloven.
([252]) Artikkel 7 i antiterrorloven.
([253]) Artikkel 7 nr. 1 i gjennomføringsdekretet til antiterrorloven.
([254]) Artikkel 7 nr. 3 i gjennomføringsdekretet til antiterrorloven.
([255]) Artikkel 8 nr. 1 i gjennomføringsdekretet til antiterrorloven.
([256]) Artikkel 9 nr. 1 i gjennomføringsdekretet til antiterrorloven. HRPO treffer beslutning om vedtakelse av anbefalinger på en selvstendig måte, men skal rapportere slike anbefalinger til lederen for antiterrorkommisjonen.
([257]) Artikkel 9 nr. 2 i gjennomføringsdekretet til antiterrorloven.
([258]) Artikkel 36 og 37 nr. 1 pkt. 16 i loven om nasjonalforsamlingen.

med organets tjenesteutøvelse, rapporterer til etterretningsutvalget (og til presidenten)([259]). Etterretningsutvalget kan også selv anmode om en rapport om en bestemt sak, som direktøren for NIS uten opphold skal svare på([260]). Vedkommende kan bare nekte å svare eller avgi vitneforklaring for etterretningsutvalget dersom det er snakk om statshemmeligheter som gjelder militære eller diplomatiske spørsmål eller spørsmål knyttet til Nord-Korea, og dersom det kan ha alvorlige konsekvenser for landets «nasjonale skjebne» dersom offentligheten får kjennskap til dette([261]). I så fall kan etterretningsutvalget anmode statsministeren om en forklaring. Dersom det ikke gis en forklaring senest sju dager etter at anmodningen er inngitt, kan det ikke lenger nektes å svare eller avgi vitneforklaring.

Dersom nasjonalforsamlingen fastslår at det har funnet sted ulovlige eller urettmessige aktiviteter, kan den anmode om at den relevante offentlige myndigheten treffer korrigerende tiltak, herunder gir erstatning, treffer disiplinære tiltak og forbedrer sine interne prosedyrer([262]). Etter en slik anmodning skal myndigheten uten opphold handle og rapportere resultatet til nasjonalforsamlingen. Det finnes særlige regler for parlamentarisk tilsyn når det gjelder bruk av kommunikasjonsbegrensende tiltak (det vil si innsamling av kommunikasjonsinnhold) i henhold til CCPA([263]). Når det gjelder det sistnevnte, kan nasjonalforsamlingen anmode lederne for etterretningsorganene om en rapport om eventuelle spesifikke kommunikasjonsbegrensende tiltak. De kan også foreta stedlige inspeksjoner av avlyttingsutstyr. Etterretningsorganer som har samlet inn, og operatører som har utlevert innholdsopplysninger for formål knyttet til nasjonal sikkerhet, skal rapportere om slik utlevering på anmodning fra nasjonalforsamlingen.

3.3.3. *Revisjons- og granskingsutvalget*

BAI utfører de samme tilsynsfunksjonene med hensyn til etterretningsorganer som på området strafferettslig håndheving (se avsnitt 2.3.2)([264]).

3.3.4. *Kommisjonen for vern av personopplysninger*

Når det gjelder behandling av opplysninger for formål knyttet til nasjonal sikkerhet, herunder i innsamlingsfasen, fører PIPC ytterligere tilsyn. Som forklart nærmere i avsnitt 1.2 omfatter dette de generelle prinsippene og forpliktelsene fastsatt i artikkel 3 og artikkel 58 nr. 4 i PIPA samt utøvelsen av individuelle rettigheter som garanteres ved artikkel 4 i PIPA. I henhold til artikkel 7-8 nr. 3 og 4 og artikkel 7-9 nr. 5 i PIPA omfatter PIPCs tilsyn også mulige overtredelser av reglene i spesifikke lover som fastsetter begrensninger og garantier for innsamling av personopplysninger, for eksempel CPPA, antiterrorloven og TBA. I betraktning av kravene i artikkel 3 nr. 1 i PIPA om lovlig og rettferdig innsamling av personopplysninger utgjør enhver overtredelse av disse lovene en overtredelse av PIPA. PIPC har dermed myndighet til å undersøke([265]) overtredelser av lovene som regulerer tilgangen til opplysninger for formål knyttet til nasjonal sikkerhet, og PIPAs regler for behandling og til å utstede anbefalinger om forbedringer, ilegge korrigerende tiltak, anbefale disiplinære tiltak og henvise potensielle lovovertredelser til relevante etterforskningsmyndigheter([266]).

3.3.5. *Den nasjonale menneskerettighetskommisjonen*

NHRC fører tilsyn med etterretningsorganer på samme måte som med andre statlige myndigheter (se avsnitt 2.3.2).

3.4. **Individuell prøvings-/klageadgang**

3.4.1. *Adgang til å klage til den ansvarlige for vern av menneskerettigheter*

Når det gjelder innsamling av personopplysninger i forbindelse med terrorbekjempelsesaktiviteter, stiller HRPO, som er opprettet under antiterrorkommisjonen, en særlig klagemulighet til rådighet. HRPO behandler sivile klager knyttet til krenking av menneskerettighetene som følge av terrorbekjempelsesaktiviteter([267]). HRPO kan anbefale korrigerende tiltak, og det relevante organet skal underrette HRPO om ethvert tiltak som er truffet for å gjennomføre en slik anbefaling. Det er intet krav om søksmålskompetanse for personer som ønsker å klage til HRPO. Som følge av dette vil HRPO behandle klagen, selv om den berørte personen ikke kan påvise en faktisk skade på tidspunktet for gjennomgåelsen av om klagen kan behandles.

([259]) Artikkel 18 i NIS-loven.
([260]) Artikkel 15 nr. 2 i NIS-loven.
([261]) Artikkel 17 nr. 2 i NIS-loven. «Statshemmeligheter» defineres som «fakta, varer eller kunnskap som klassifiseres som statshemmeligheter, og som et begrenset antall personer har tilgang til, og som for å unngå alvorlige konsekvenser for den nasjonale sikkerheten ikke skal utleveres til et annet land eller en annen organisasjon, se artikkel 13 nr. 4 i NIS-loven.
([262]) Artikkel 16 nr. 2 i loven om inspeksjon og gransking av statsforvaltningen.
([263]) Artikkel 15 i CPPA.
([264]) Som for nasjonalforsamlingens etterretningsutvalg kan direktøren for NIS bare nekte å svare BAI dersom det er snakk om statshemmeligheter, og dersom det vil kunne ha alvorlige konsekvenser for den nasjonale sikkerheten dersom offentligheten får kjennskap til dette (artikkel 13 nr. 1 i NIS-loven).
([265]) Artikkel 63 i PIPA.
([266]) Artikkel 61 nr. 2, artikkel 65 nr. 1, artikkel 65 nr. 2 og artikkel 64 nr. 4 i PIPA.
([267]) Artikkel 8 nr. 1 pkt. 2 i gjennomføringsdekretet til antiterrorloven.

3.4.2. *Prøvingsmekanismer i henhold til PIPA*

Enkeltpersoner kan utøve sin rett til innsyn i, retting og sletting og til å få innstilt behandlingen i henhold til PIPA av personopplysninger som behandles for formål knyttet til nasjonal sikkerhet([268]). Anmodninger om å utøve disse rettighetene kan inngis direkte til etterretningsorganet eller indirekte via PIPC. Etterretningsorganet kan begrense eller nekte utøvelsen av en slik rettighet i den grad og så lenge det er nødvendig og forholdsmessig for å beskytte et viktig mål av allmenn interesse (for eksempel i den grad og så lenge å gi rettigheten vil bringe en pågående etterforskning i fare eller true den nasjonale sikkerheten), eller dersom det å gi rettigheten kan skade en tredjeparts liv eller legeme. Dersom anmodningen avslås eller begrenses, skal den aktuelle personen uten opphold underrettes om grunnene til dette.

I samsvar med artikkel 58 nr. 4 i PIPA (krav om å sikre egnet behandling av individuelle klager) og artikkel 4 nr. 5 i PIPA (retten til egnet erstatning for enhver skade som følger av behandlingen av personopplysninger, gjennom en rask og rettferdig prosedyre), har enkeltpersoner dessuten rett til prøving. Dette omfatter retten til å rapportere om en påstått overtredelse til personverntelefontjenesten som drives av Republikken Koreas byrå for internett og sikkerhet, og til å inngi en klage til PIPC([269]). Disse rettsmidlene er tilgjengelige både ved mulige overtredelser av reglene i spesifikke lover der det er fastsatt særlige begrensninger og garantier for innsamling av personopplysninger for formål knyttet til nasjonalsikkerhet, og i PIPA. Som forklart i melding 2021-1 kan en EU-borger inngi en klage til PIPC via sin nasjonale personvernmyndighet. Da vil PIPC underrette den aktuelle personen via den nasjonale personvernmyndigheten når undersøkelsen er avsluttet (herunder, dersom det er relevant, med opplysninger om de korrigerende tiltakene som er truffet). PIPCs beslutninger eller unnlatelse av å handle kan bringes inn for de sørkoreanske domstolene i henhold til forvaltningsprosessloven.

3.4.3. *Klageadgang ved den nasjonale menneskerettighetskommisjonen*

Muligheten for å oppnå individuell prøvings-/klageadgang ved NHRC gjelder på samme måte for etterretningsorganer som for andre statlige myndigheter (se avsnitt 2.4.2).

3.4.4. *Rettslig prøving*

Som med strafferettshåndhevende myndigheters aktiviteter har enkeltpersoner forskjellige muligheter til å oppnå rettslig prøving mot etterretningsorganer i forbindelse med overtredelser av begrensningene og garantiene nevnt over.

For det første kan enkeltpersoner oppnå skadeserstatning i henhold til loven om statlig erstatning. I en sak er det for eksempel gitt erstatning for ulovlig overvåking foretatt av forsvarsstøttekommandoen (forløperen til forsvarssikkerhetskommandoen)([270]).

For det andre gir forvaltningsprosessloven enkeltpersoner mulighet til å bestride forvaltningsorganers, herunder etterretningsorganers, disposisjoner og unnlatelser([271]).

Enkeltpersoner kan også inngi en forfatningsmessig klage til forfatningsdomstolen mot tiltak truffet av etterretningsorganer på grunnlag av loven om forfatningsdomstolen.

([268]) Artikkel 3 nr. 5 og artikkel 4 nr. 1, 3 og 4 i PIPA.
([269]) Artikkel 62 og artikkel 63 nr. 2 i PIPA.
([270]) Høyesteretts avgjørelse 96Da42789 av 24. juli 1998.
([271]) Artikkel 3 og 4 i forvaltningsprosessloven.