KOMMISJONSFORORDNING (EU) NR. 611/2013 **2018/EØS/73/33**

av 24. juni 2013

om tiltak som får anvendelse på melding av brudd på personopplysningssikkerheten i henhold til europaparlaments- og rådsdirektiv 2002/58/EF om personvern og elektronisk kommunikasjon(*)

EUROPAKOMMISJONEN HAR

under henvisning til traktaten om Den europeiske unions virkemåte,

under henvisning til europaparlaments- og rådsdirektiv 2002/58/EF av 12. juli 2002 om behandling av personopplysninger og personvern i sektoren for elektronisk kommunikasjon (direktivet om personvern og elektronisk kommunikasjon)([1]), særlig artikkel 4 nr. 5,

etter samråd med Den europeiske unions byrå for nett- og informasjonssikkerhet (ENISA),

etter samråd med arbeidsgruppen for personvern i forbindelse med behandling av personopplysninger nedsatt ved artikkel 29 i europaparlaments- og rådsdirektiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger([2]) («artikkel 29-arbeidsgruppen»),

etter samråd med EUs datatilsyn og

ut fra følgende betraktninger:

1) Ved direktiv 2002/58/EF harmoniseres de nasjonale bestemmelser som er nødvendige for å sikre et ensartet nivå for beskyttelse av grunnleggende rettigheter og friheter, særlig retten til personvern og fortrolighet, med hensyn til behandling av personopplysninger i sektoren for elektronisk kommunikasjon, og for å sikre fri utveksling av slike opplysninger og fri bevegelighet for elektronisk kommunikasjonsutstyr og elektroniske kommunikasjonstjenester i Unionen.

2) I henhold til artikkel 4 i direktiv 2002/58/EF skal tilbydere av offentlig tilgjengelige elektroniske kommunikasjonstjenester underrette vedkommende nasjonale myndigheter, og i noen tilfeller også de berørte abonnenter og privatpersoner, om brudd på personopplysningssikkerheten. Brudd på personopplysningssikkerheten defineres i artikkel 2 bokstav i) i direktiv 2002/58/EF som et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet i forbindelse med levering av en offentlig tilgjengelig elektronisk kommunikasjonstjeneste i Unionen.

3) For å sikre ensartet gjennomføring av tiltakene nevnt i artikkel 4 nr. 2, 3 og 4 i direktiv 2002/58/EF gir artikkel 4 nr. 5 i nevnte direktiv Kommisjonen myndighet til å vedta tekniske gjennomføringstiltak vedrørende omstendigheter, format og framgangsmåter som skal gjelde for opplysnings- og meldekravene omhandlet i nevnte artikkel.

4) Avvikende nasjonale krav på dette området kan føre til rettslig usikkerhet, mer sammensatte og tungvinte framgangsmåter og betydelige administrasjonskostnader for tilbydere som driver virksomhet over landegrensene. Kommisjonen mener derfor at det er nødvendig å vedta nevnte tekniske gjennomføringstiltak.

5) Denne forordning er begrenset til melding av brudd på personopplysningssikkerheten og omfatter derfor ikke tekniske gjennomføringstiltak med hensyn til artikkel 4 nr. 2 i direktiv 2002/58/EF om underretning av abonnenter dersom det foreligger en særlig fare for brudd på nettsikkerheten.

6) Det framgår av artikkel 4 nr. 3 første ledd i direktiv 2002/58/EF at tilbydere skal melde alle brudd på personopplysningssikkerheten til vedkommende nasjonale myndighet. Tilbyderen bør derfor ikke selv kunne avgjøre om melding skal gis til vedkommende nasjonale myndighet eller ikke. Dette bør imidlertid ikke hindre den berørte vedkommende nasjonale myndighet i å prioritere gransking av visse brudd på en måte som den finner hensiktsmessig i samsvar med gjeldende lovgivning, og å treffe nødvendige tiltak for å unngå over- eller underrapportering av brudd på personopplysningssikkerheten.

7) Det bør innføres et system for melding av brudd på personopplysningssikkerheten til vedkommende nasjonale myndighet som, dersom visse vilkår er oppfylt, består av forskjellige faser med frister for hver enkelt fase. Hensikten med dette systemet er å sikre at vedkommende nasjonale myndighet underrettes så tidlig og utførlig som mulig, men uten at tilbyderen hindres unødig i å granske bruddet eller treffe nødvendige tiltak for å utbedre og begrense konsekvensene av det.

(*) Denne unionsrettsakten, kunngjort i EUT L 173 av 26.6.2013, s. 2, er omhandlet i EØS-komiteens beslutning nr. 154/2016 av 8. juli 2016 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester), se EØS-tillegget til *Den europeiske unions tidende* nr. 16 av 15.3.2018, s. 33.

([1]) EFT L 201 av 31.7.2002, s. 37.

([2]) EFT L 281 av 23.11.1995, s. 31.

8) Verken mistanke om at et brudd på personopplysningssikkerheten har funnet sted, eller påvisning av en hendelse uten at det foreligger tilstrekkelige opplysninger, til tross for at tilbyder gjør sitt ytterste for å innhente disse, er tilstrekkelig til å anse et brudd på personopplysningssikkerheten som påvist i henhold til denne forordning. Det bør tas særlig hensyn til om de opplysninger som er omhandlet i vedlegg I, foreligger.

9) Innenfor rammen av anvendelsen av denne forordning bør berørte vedkommende nasjonale myndigheter samarbeide i tilfeller der brudd på personopplysningssikkerheten har tverrnasjonale konsekvenser.

10) Denne forordning inneholder ingen nærmere spesifisering av fortegnelsen over brudd på personopplysningssikkerheten som tilbydere skal føre, ettersom artikkel 4 i direktiv 2002/58/EF inneholder en uttømmende beskrivelse av hva den skal inneholde. Tilbydere kan imidlertid anvende denne forordning for å fastsette fortegnelsens format.

11) Alle vedkommende nasjonale myndigheter bør gjøre sikre elektroniske midler tilgjengelig for tilbydere, slik at brudd på personopplysningssikkerheten kan meldes i et felles format basert på en standard, for eksempel XML, som inneholder opplysningene angitt i vedlegg I på de relevante språkene, og slik at alle tilbydere i Unionen kan følge en ensartet framgangsmåte for melding, uavhengig av hvor de befinner seg eller hvor bruddet på personopplysningssikkerheten fant sted. I denne forbindelse bør Kommisjonen fremme innføringen av de sikre elektroniske midlene ved å innkalle vedkommende nasjonale myndigheter til møter ved behov.

12) Ved vurderingen av om et brudd på personopplysningssikkerheten kan antas å sette en abonnents eller en privatpersons personvern eller personopplysninger i fare, bør det tas særlig hensyn til de berørte personopplysningenes art og innhold, særlig dersom opplysningene er av finansiell art, for eksempel kredittkort- og bankkontoopplysninger, særlige kategorier av opplysninger nevnt i artikkel 8 nr. 1 i direktiv 95/46/EF og visse opplysninger som særlig er knyttet til levering av telefoni- eller internettjenester, dvs. e-postopplysninger, lokaliseringsopplysninger, internettloggfiler, nettleserhistorikk og spesifiserte samtalelister.

13) I særlige tilfeller bør tilbyderen kunne utsette å underrette abonnenten eller privatpersonen dersom en slik underretning kan bringe granskingen av bruddet på personopplysningssikkerheten i fare. I denne forbindelse kan særlige tilfeller omfatte strafferettslig etterforskning og andre brudd på personopplysningssikkerheten som ikke utgjør alvorlige lovbrudd, men som kan berettige at underretningen utsettes. I alle tilfeller bør det være opp til vedkommende nasjonale myndighet å vurdere, ut fra hvert enkelt tilfelle og i lys av omstendighetene, om det skal samtykkes i utsettelsen, eller om det skal kreves at underretning gis.

14) Tilbydere forventes å ha kontaktopplysninger til sine abonnenter ettersom de har et direkte kontraktsforhold til disse, men slike opplysninger foreligger ikke alltid for andre privatpersoner som berøres av et brudd på personopplysningssikkerheten. I slike tilfeller bør tilbyderen ha rett til å underrette nevnte privatpersoner først gjennom annonser i større nasjonale eller regionale medier, for eksempel aviser, og deretter underrette hver enkelt person snarest mulig som fastsatt i denne forordning. Tilbyderen plikter derfor ikke å gi underretning via media, men kan velge å gjøre dette mens identifiseringen av alle berørte privatpersoner pågår.

15) Opplysningene om bruddet bør bare omhandle bruddet og ikke andre emner. Eksempelvis bør ikke orientering om et brudd på personopplysningssikkerheten i en vanlig faktura anses som en hensiktsmessig måte å underrette om slike brudd på.

16) Ved denne forordning fastsettes det ikke særlige tekniske beskyttelsestiltak som berettiger et unntak fra plikten til å underrette abonnenter eller privatpersoner om brudd på personopplysningssikkerheten, ettersom slike tiltak kan endres over tid i takt med den teknologiske utvikling. Kommisjonen bør imidlertid kunne offentliggjøre en veiledende liste over slike særlige tekniske beskyttelsestiltak i henhold til gjeldende praksis.

17) Bruk av kryptering eller hashing bør ikke i seg selv anses som tilstrekkelig til at tilbydere generelt kan hevde at de har oppfylt den generelle sikkerhetsforpliktelsen fastsatt i artikkel 17 i direktiv 95/46/EF. I denne forbindelse bør tilbydere også iverksette egnede organisatoriske og tekniske tiltak for å forebygge, påvise og hindre brudd på personopplysningssikkerheten. Tilbydere bør vurdere eventuelle farer som gjenstår etter at kontroller er gjennomført, for å få en forståelse av hvor det potensielt kan oppstå brudd på personopplysningssikkerheten.

18) Dersom tilbyderen benytter en annen tilbyder til å utføre deler av tjenesten, for eksempel i forbindelse med fakturering eller administrative oppgaver, bør nevnte andre tilbyder, som ikke har et direkte kontraktsforhold til sluttbrukeren, ikke være forpliktet til å underrette om brudd på personopplysningssikkerheten. Vedkommende bør isteden varsle og underrette tilbyderen som vedkommende har et direkte kontraktsforhold til. Dette bør også gjelde i forbindelse med engroslevering av

elektroniske kommunikasjonstjenester der tilbyderen i grossistleddet vanligvis ikke har et direkte kontraktsforhold til sluttbrukeren.

19) Ved direktiv 95/46/EF fastsettes det en generell ramme for vern av personopplysninger i Den europeiske union. Kommisjonen har framlagt et forslag til europaparlaments- og rådsforordning som skal erstatte direktiv 95/46/EF (personvernforordningen). I den foreslåtte personvernforordningen innføres det en plikt for alle behandlingsansvarlige til å melde brudd på personopplysningssikkerheten med utgangspunkt i artikkel 4 nr. 3 i direktiv 2002/58/EF. Denne kommisjonsforordning samsvarer fullt ut med dette foreslåtte tiltak.

20) I den foreslåtte personvernforordningen gjøres det også et begrenset antall tekniske tilpasninger av direktiv 2002/58/EF for å ta høyde for at direktiv 95/46/EF omgjøres til en forordning. Den nye forordnings materielle rettsvirkninger for direktiv 2002/58/EF vil bli gjennomgått av Kommisjonen.

21) Anvendelsen av denne forordning bør gjennomgås på nytt tre år etter at den er trådt i kraft, og forordningens innhold bør gjennomgås på nytt på grunnlag av den rettslige rammen som gjelder på nevnte tidspunkt, herunder den foreslåtte personvernforordningen. Når det er mulig, bør gjennomgåelsen av denne forordning knyttes til en eventuell fremtidig gjennomgåelse av direktiv 2002/58/EF.

22) Anvendelsen av denne forordning kan blant annet vurderes på grunnlag av vedkommende nasjonale myndigheters statistikk over brudd på personopplysningssikkerheten som de mottar melding om. Nevnte statistikk kan for eksempel omfatte opplysninger om antall brudd på personopplysningssikkerheten som er meldt til vedkommende nasjonale myndighet, antall brudd på personopplysningssikkerheten som abonnenter eller privatpersoner er blitt underrettet om, tiden det har tatt å utbedre bruddet på personopplysningssikkerheten, og om det er truffet tekniske beskyttelsestiltak. Nevnte statistikk bør gi Kommisjonen og medlemsstatene sammenhengende og sammenlignbare statistiske opplysninger og bør ikke avsløre identiteten til tilbyderen som gir meldingen, eller til berørte abonnenter eller privatpersoner. For dette formål kan kommisjonen også avholde jevnlige møter med vedkommende nasjonale myndigheter og andre berørte parter.

23) Tiltakene fastsatt i denne forordning er i samsvar med uttalelse fra Kommunikasjonskomiteen.

VEDTATT DENNE FORORDNING:

Artikkel 1

Virkeområde

Denne forordning får anvendelse på melding av brudd på personopplysningssikkerheten som gis av tilbydere av offentlig tilgjengelige elektroniske kommunikasjonstjenester («tilbyderen»).

Artikkel 2

Melding til vedkommende nasjonale myndighet

1. Tilbyderen skal melde alle brudd på personopplysningssikkerheten til vedkommende nasjonale myndighet.

2. Når det er mulig, skal tilbyderen melde bruddet på personopplysningssikkerheten til vedkommende nasjonale myndighet senest 24 timer etter at bruddet er påvist.

Tilbyderen skal i sin melding til vedkommende nasjonale myndighet oppgi opplysningene angitt i vedlegg I.

Et brudd på personopplysningssikkerheten skal anses for å være påvist når tilbyderen har fått tilstrekkelig kjennskap til at det har inntruffet en sikkerhetshendelse som har ført til at personopplysninger settes i fare, i den grad at det berettiger en melding i samsvar med denne forordning.

3. Dersom ikke alle opplysningene angitt i vedlegg I foreligger, og det kreves ytterligere gransking av bruddet på personopplysningssikkerheten, skal tilbyderen ha rett til å inngi en innledende melding til vedkommende nasjonale myndighet senest 24 timer etter at bruddet på personopplysningssikkerheten er påvist. Den innledende meldingen til vedkommende nasjonale myndighet skal inneholde opplysningene angitt i vedlegg I del 1. Tilbyderen skal inngi en ny melding til vedkommende nasjonale myndighet snarest mulig, og senest tre dager etter den innledende meldingen. Melding nummer to skal inneholde opplysningene angitt i vedlegg I del 2 og, ved behov, en ajourføring av opplysningene som allerede er gitt.

Dersom tilbyderen til tross for sin gransking ikke er i stand til å framlegge alle opplysningene senest tre dager etter den innledende meldingen, skal tilbyderen framlegge de opplysninger vedkommende har tilgjengelig, innen nevnte frist, og gi vedkommende nasjonale myndighet en gyldig begrunnelse for den sene meldingen av de øvrige opplysningene. Tilbyderen skal snarest mulig framlegge de øvrige opplysningene for vedkommende nasjonale myndighet og, dersom det er nødvendig, ajourføre opplysningene som allerede er gitt.

4. Vedkommende nasjonale myndighet skal stille til rådighet et sikkert elektronisk middel for melding av brudd på personopplysningssikkerheten, samt opplysninger om framgangsmåter for bruk av og tilgang til dette, for alle tilbydere som er etablert i den berørte medlemsstat. Ved behov skal Kommisjonen innkalle til møter med vedkommende nasjonale myndigheter for å fremme anvendelsen av denne bestemmelse.

5. Dersom bruddet på personopplysningssikkerheten påvirker abonnenter eller privatpersoner fra andre medlemsstater enn den medlemsstat der bruddet er meldt til vedkommende nasjonale myndighet, skal vedkommende nasjonale myndighet underrette de andre berørte nasjonale myndigheter.

For å fremme anvendelsen av denne bestemmelse skal Kommisjonen opprette og ajourføre en liste over vedkommende nasjonale myndigheter og egnede kontaktpunkter.

Artikkel 3

Underretning til abonnenten eller privatpersonen

1. Dersom bruddet på personopplysningssikkerheten kan forventes å sette en abonnents eller en privatpersons personvern eller personopplysninger i fare, skal tilbyderen, i tillegg til meldingen nevnt i artikkel 2, også underrette abonnenten eller privatpersonen om bruddet.

2. Hvorvidt det er sannsynlig at et brudd på personopplysningssikkerheten vil sette en abonnents eller privatpersons personvern eller personopplysninger i fare, skal vurderes ved å ta særlig hensyn til følgende forhold:

a) De berørte personopplysningenes art og innhold, særlig dersom opplysningene er av finansiell art, særlige kategorier av opplysninger nevnt i artikkel 8 nr. 1 i direktiv 95/46/EF samt lokaliseringsopplysninger, internettloggfiler, nettleserhistorikk, e-postopplysninger og spesifiserte samtalelister.

b) De sannsynlige konsekvensene som bruddet på personopplysningssikkerheten vil ha for den berørte abonnent eller privatperson, særlig dersom bruddet kan føre til identitetstyveri eller bedrageri, fysisk skade, psykisk belastning, fornedrelse eller skade på omdømme.

c) Omstendighetene rundt bruddet på personopplysningssikkerheten, særlig dersom opplysninger er blitt stjålet, eller dersom tilbyderen kjenner til at opplysningene har kommet en uvedkommende tredjepart i hende.

3. Abonnenten eller privatpersonen skal underrettes snarest mulig etter at bruddet på personopplysningssikkerheten er påvist, som fastsatt i artikkel 2 nr. 2 tredje ledd. Underretningen skal gis uavhengig av meldingen av bruddet på personopplysningssikkerheten til vedkommende nasjonale myndighet nevnt i artikkel 2.

4. Tilbyderen skal i sin underretning til abonnenten eller privatpersonen gi opplysningene angitt i vedlegg II. Underretningen til abonnenten eller privatpersonen skal formuleres på et tydelig og lettfattelig språk. Tilbyderen skal ikke bruke underretningen som en anledning til å markedsføre eller reklamere for nye tjenester eller tilleggstjenester.

5. I særlige tilfeller, dersom underretningen til abonnenten eller privatpersonen kan bringe granskingen av bruddet på personopplysningssikkerheten i fare, skal tilbyderen, etter å ha innhentet samtykke fra vedkommende nasjonale myndighet, ha rett til å utsette underretning av abonnenten eller privatpersonen fram til vedkommende nasjonale myndighet anser det som mulig å underrette om bruddet på personopplysningssikkerheten i samsvar med denne artikkel.

6. Tilbyderen skal underrette abonnenten eller privatpersonen om bruddet på personopplysningssikkerheten ved hjelp av kommunikasjonsmidler som sikrer raskt mottak av opplysningene, og som er hensiktsmessig sikret i henhold til det nåværende utviklingstrinn i teknikken. Opplysningene om bruddet skal bare omhandle bruddet og ikke inneholde opplysninger om andre emner.

7. Dersom tilbyderen som har et direkte kontraktsforhold til sluttbrukeren, til tross for rimelige anstrengelser ikke er i stand til å identifisere alle de privatpersoner som trolig vil bli rammet av bruddet på personopplysningssikkerheten, innen tidsfristen angitt i nr. 3, kan tilbyderen underrette nevnte privatpersoner gjennom annonser i større nasjonale eller regionale medier i de berørte medlemsstater innen nevnte tidsfrist. Annonsene skal inneholde opplysningene angitt i vedlegg II, ved behov i sammenfattet form. I dette tilfellet skal tilbyderen fortsette å gjøre alle rimelige anstrengelser for å identifisere nevnte privatpersoner og snarest mulig gi dem opplysningene angitt i vedlegg II.

Artikkel 4

Tekniske beskyttelsestiltak

1. Som unntak fra artikkel 3 nr. 1 er det ikke nødvendig å underrette den berørte abonnent eller privatperson om et brudd på personopplysningssikkerheten dersom vedkommende nasjonale myndighet finner det tilfredsstillende godtgjort at tilbyderen har iverksatt hensiktsmessige tekniske beskyttelsestiltak, og at disse tiltakene er anvendt på opplysningene berørt av sikkerhetsbruddet. Slike tekniske beskyttelsestiltak skal gjøre opplysningene uleselige for enhver som ikke har tilgangstillatelse til dem.

2. Opplysningene skal anses som uleselige dersom

a) de er blitt kryptert på en sikker måte ved hjelp av en standardisert algoritme, og nøkkelen som brukes til dekryptering, ikke er blitt kompromittert i et sikkerhetsbrudd og er blitt generert på en slik måte at den ikke kan gjenfinnes med eksisterende teknologiske midler av personer som ikke har tillatelse til å bruke den, eller

b) de er blitt erstattet av en hash-verdi beregnet med en standardisert kryptografisk hash-funksjon med nøkkel, og nøkkelen som er brukt til hashing, ikke er blitt kompromittert i et sikkerhetsbrudd og er blitt generert på en slik måte at den ikke kan gjenfinnes med eksisterende teknologiske midler av personer som ikke har tillatelse til å bruke den.

3. Kommisjonen kan, etter å ha rådført seg med vedkommende nasjonale myndigheter via artikkel 29 -arbeidsgruppen, Den europeiske unions byrå for nett- og informasjonssikkerhet og EUs datatilsyn, offentliggjøre en veiledende liste over egnede tekniske beskyttelsestiltak som nevnt i nr. 1 i samsvar med gjeldende praksis.

Artikkel 5

Bruk av en annen tilbyder

Dersom det inngås kontrakt med en annen tilbyder som ikke har et direkte kontraktsforhold til abonnentene, om levering av deler av den elektroniske kommunikasjonstjenesten, skal nevnte andre tilbyder umiddelbart underrette den tilbyder som har engasjert vedkommende, om eventuelle brudd på personopplysningssikkerheten.

Artikkel 6

Rapportering og ny gjennomgåelse

Innen tre år etter ikrafttredelsen av denne forordning skal Kommisjonen framlegge en rapport om denne forordnings anvendelse, virkning og innvirkning på tilbydere, abonnenter og privatpersoner. Kommisjonen skal foreta en ny gjennomgåelse av denne forordning på grunnlag av nevnte rapport.

Artikkel 7

Ikrafttredelse

Denne forordning trer i kraft 25. august 2013.

Denne forordning er bindende i alle deler og kommer direkte til anvendelse i alle medlemsstater.

Utferdiget i Brussel 24. juni 2013.

For Kommisjonen

José Manuel BARROSO

President

VEDLEGG I

Innhold i meldingen til vedkommende nasjonale myndighet

Del 1

Identifikasjon av tilbyderen

1. Tilbyderens navn
2. Identiteten og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der flere opplysninger kan innhentes
3. Hvorvidt det dreier seg om en første eller andre melding

Innledende opplysninger om bruddet på personopplysningssikkerheten (opplysningene kompletteres i senere meldinger dersom det er relevant)

4. Dato og tidspunkt for hendelsen (dersom dette er kjent; ved behov kan det gis et anslag) og for påvisning av hendelsen
5. Omstendighetene rundt bruddet på personopplysningssikkerheten (f.eks. tap, tyveri, kopiering)
6. De berørte personopplysningenes art og innhold
7. Tekniske og organisatoriske tiltak som tilbyderen har truffet (eller kommer til å treffe) med hensyn til de berørte personopplysningene
8. Relevant bruk av andre tilbydere (dersom dette er relevant)

Del 2

Ytterligere opplysninger om bruddet på personopplysningssikkerheten

9. Sammendrag av hendelsen som forårsaket bruddet på personopplysningssikkerheten (herunder det fysiske stedet der bruddet oppsto samt lagringsmediet som ble brukt):
10. Antall berørte abonnenter eller privatpersoner
11. Potensielle konsekvenser og potensielle skadevirkninger for abonnenter eller privatpersoner
12. Tekniske og organisatoriske tiltak som tilbyderen har truffet for å redusere potensielle skadevirkninger

Eventuell ytterligere underretning til abonnenter eller privatpersoner

13. Underretningens innhold
14. Kommunikasjonsmidler som er brukt
15. Antall abonnenter eller privatpersoner som er blitt underrettet

Eventuelle tverrnasjonale forhold

16. Brudd på personopplysningssikkerheten som berører abonnenter eller privatpersoner i andre medlemsstater
17. Melding til andre vedkommende nasjonale myndigheter

———

VEDLEGG II

Innhold i underretningen til abonnenten eller privatpersonen

1. Tilbyderens navn
2. Identiteten og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der flere opplysninger kan innhentes
3. Sammendrag av hendelsen som forårsaket bruddet på personopplysningssikkerheten
4. Anslått dato for hendelsen
5. De berørte personopplysningenes art og innhold som nevnt i artikkel 3 nr. 2
6. Sannsynlige konsekvenser av bruddet på personopplysningssikkerheten for den berørte abonnenten eller privatpersonen som nevnt i artikkel 3 nr. 2
7. Omstendighetene rundt bruddet på personopplysningssikkerheten som nevnt i artikkel 3 nr. 2
8. Tiltak truffet av tilbyderen for å håndtere bruddet på personopplysningssikkerheten
9. Tiltak anbefalt av tilbyderen for å redusere mulige skadevirkninger