FÖRORDNINGAR

KOMMISSIONENS FÖRORDNING (EU) nr 611/2013

av den 24 juni 2013

om åtgärder tillämpliga på anmälan av personuppgiftsbrott enligt Europaparlamentets och rådets direktiv 2002/58/EG vad gäller personlig integritet och elektronisk kommunikation

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets direktiv 2002/58/EG av den 12 juli 2002 om behandling av personuppgifter och integritetsskydd inom sektorn för elektronisk kommunikation (direktiv om integritet och elektronisk kommunikation) ([1]), särskilt artikel 4.5,

efter att ha samrått med Europeiska byrån för nät- och informationssäkerhet (Enisa),

efter att ha samrått med arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter, som inrättades genom artikel 29 i Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter ([2]) (artikel 29-gruppen),

efter att ha samrått med Europeiska datatillsynsmannen, och

av följande skäl:

(1) Genom direktiv 2002/58/EG möjliggörs en harmonisering av nationella bestämmelser för att säkerställa ett likvärdigt skydd av de grundläggande fri- och rättigheterna, i synnerhet rätten till personlig integritet och konfidentialitet, när det gäller behandling av personuppgifter inom sektorn för elektronisk kommunikation, samt för att säkerställa fri rörlighet för sådana uppgifter och för utrustning och tjänster avseende elektronisk kommunikation inom unionen.

(2) Enligt artikel 4 i direktiv 2002/58/EG ska leverantören av en allmänt tillgänglig elektronisk kommunikationstjänst anmäla personuppgiftsbrott till den behöriga nationella myndigheten och i vissa fall även till berörda abonnenter och privatpersoner. Personuppgiftsbrott definieras i artikel 2 i i direktiv 2002/58/EG som ett brott mot säkerhetsbestämmelserna som leder till oavsiktlig eller olaglig utplåning, förlust, ändring, otillåtet avslöjande eller åtkomst av personuppgifter som överförs, lagras eller på annat sätt behandlas i samband med tillhandahållandet av allmänt tillgänglig elektronisk kommunikationstjänst inom unionen.

(3) För att säkerställa ett konsekvent genomförande av de åtgärder som avses i 4.2–4.4 i direktiv 2002/58/EG får kommissionen enligt artikel 4.5 i samma direktiv anta tekniska genomförandeåtgärder avseende omständigheter, format och förfaranden som kan tillämpas för de informations- och anmälningskrav som avses i den artikeln.

(4) Olika nationella krav i detta hänseende kan leda till rättsosäkerhet, mer komplicerade och betungande förfaranden och betydande administrativa kostnader för leverantörer med gränsöverskridande verksamhet. Kommissionen anser därför att sådana tekniska genomförandeåtgärder bör antas.

(5) Denna förordning är begränsad till anmälan av personuppgiftsbrott och omfattar därför inte några tekniska genomförandeåtgärder avseende artikel 4.2 i direktiv 2002/58/EG vad gäller information till abonnenterna om det föreligger särskilda risker för brott mot nätsäkerheten.

(6) Av artikel 4.3 första stycket i direktiv 2002/58/EG framgår att leverantören ska anmäla alla personuppgiftsbrott till den behöriga nationella myndigheten. Leverantören bör därför inte själv få avgöra om den behöriga nationella myndigheten ska underrättas. Detta bör dock inte hindra den berörda behöriga nationella myndigheten från att prioritera undersökning av vissa brott på lämpligt sätt i enlighet med tillämplig lagstiftning och vidta åtgärder som är nödvändiga för att undvika över- eller underrapportering av personuppgiftsbrott.

(7) Det är lämpligt att införa ett system för anmälan av personuppgiftsbrott till den behöriga nationella myndigheten som består, om vissa villkor är uppfyllda, av olika steg med tidsgränser för vart och ett av stegen. Systemet är tänkt att garantera att den behöriga nationella myndigheten informeras så tidigt och fullständigt som möjligt, dock utan att hindra leverantören från att utreda brottet och vidta nödvändiga åtgärder för att begränsa brottet och åtgärda följderna av det.

([1]) EGT L 201, 31.7.2002, s. 37.
([2]) EGT L 281, 23.11.1995, s. 31.

(8) Det räcker varken med enbart en misstanke om att personuppgiftsbrott inträffat eller med enbart ett avslöjande av en incident utan att det finns tillräcklig information, trots att en leverantör gör sitt bästa för att få fram sådan information, för att det ska anses att ett personuppgiftsbrott har upptäckts i enlighet med denna förordning. Särskild hänsyn bör tas till tillgängligheten i fråga om den information som avses i bilaga I.

(9) Vid tillämpning av denna förordning bör de berörda behöriga nationella myndigheterna samarbeta om personuppgiftsbrottet har gränsöverskridande inslag.

(10) Denna förordning innehåller inga ytterligare specifikationer av förteckningar över personuppgiftsbrott som leverantörer ska föra, eftersom artikel 4 i direktiv 2002/58/EG ger en uttömmande beskrivning av förteckningarnas innehåll. Leverantörer kan dock hänvisa till denna förordning för att fastställa förteckningens format.

(11) Alla behöriga nationella myndigheter bör tillhandahålla ett säkert sätt för leverantörerna att på elektronisk väg anmäla personuppgiftsbrott i ett gemensamt format, baserat på en standard som t.ex. XML, som innehåller alla uppgifter som anges i bilaga I på de berörda språken, så att alla leverantörer inom unionen kan använda ett likadant anmälningsförfarande oavsett var de är lokaliserade eller var personuppgiftsbrottet inträffat. I det sammanhanget bör kommissionen underlätta genomförandet av säkra sätt att på elektronisk väg anmäla personuppgiftsbrott genom att sammankalla möten med de behöriga nationella myndigheterna när det är nödvändigt.

(12) Vid bedömning av om ett personuppgiftsbrott kan antas inverka menligt på en abonnents eller en enskild persons personuppgifter eller integritet ska hänsyn i synnerhet tas till de berörda personuppgifternas art och innehåll, särskilt om uppgifterna rör finansiell information avseende t.ex. kreditkort och bankkonton, särskilda kategorier av uppgifter enligt artikel 8.1 i direktiv 95/46/EG och vissa uppgifter som specifikt rör tillhandahållandet av teletjänster eller internettjänster, dvs. e-post, lokaliseringsuppgifter, internetloggar, webbläsarhistorik och specificerade samtalslistor.

(13) Leverantören bör ha rätt att under exceptionella omständigheter skjuta upp anmälan till abonnenten eller privatpersonen, om en sådan anmälan kan medföra att en korrekt utredning av personuppgiftsbrottet äventyras. I detta sammanhang kan exceptionella omständigheter inbegripa brottsutredningar samt andra personuppgiftsbrott som inte innebär ett allvarligt brott och för vilka det kan vara lämpligt att skjuta upp anmälan. Det bör dock alltid vara den behöriga nationella myndigheten som i varje enskilt fall och mot bakgrund av omständigheterna bedömer om uppskjutandet godkänns eller en anmälan krävs.

(14) Leverantörerna bör ha kontaktuppgifter för sina abonnenter med tanke på direkta kontraktsförhållande, men sådana uppgifter finns kanske inte nödvändigtvis för andra enskilda personer på vilka personuppgiftsbrottet inverkar menligt. I sådana fall bör leverantören ha rätt att först underrätta dessa privatpersoner genom annonser i större nationella eller regionala medier, som tidningar, vilket snarast möjligt bör följas upp med en individuell anmälan i enlighet med denna förordning. Detta innebär att leverantören i sig inte är skyldig att ge underrättelser via medier, utan snarare kan välja att sköta underrättelsen på det viset under tiden som den hittar alla privatpersoner som berörs.

(15) Informationen om personuppgiftsbrottet bör endast behandla själva brottet och inte kopplas till information om andra ämnen. Information om ett personuppgiftsbrott som lämnas på en vanlig faktura bör t.ex. inte anses som ett lämpligt sätt att anmäla ett personuppgiftsbrott.

(16) Denna förordning omfattar inte några särskilda tekniska skyddsåtgärder som motiverar undantag från skyldigheten att anmäla personuppgiftsbrott till abonnenter eller enskilda personer, eftersom sådana kan ändras i takt med den tekniska utvecklingen. Kommissionen bör dock offentliggöra en vägledande förteckning över sådana särskilda tekniska skyddsåtgärder i enlighet med rådande praxis.

(17) Det bör inte anses tillräckligt med införande av kryptering eller hashteknik för att leverantörer generellt ska kunna hävda att de har uppfyllt de allmänna säkerhetskraven enligt artikel 17 i direktiv 95/46/EG. I detta hänseende bör leverantörerna också vidta lämpliga organisatoriska och tekniska åtgärder för att förebygga, avslöja och stoppa personuppgiftsbrott. Leverantörer bör analysera de eventuella risker som kvarstår efter att kontrollerna har genomförts för att förstå var personuppgiftsbrott skulle kunna inträffa.

(18) Om leverantörer använder en annan leverantör för att utföra delar av tjänsten, till exempel när det gäller fakturering eller förvaltningsuppgifter, bör denna andra

leverantör, som inte har något direkt kontraktsförhållande med slutanvändaren, inte vara skyldig att utfärda anmälningar i fråga om personuppgiftsbrott. Den bör i stället varsko och informera leverantören med vilken den har ett direkt kontraktsförhållande. Det bör även gälla i fråga om tillhandahållande av elektroniska kommunikationstjänster i grossistledet, när vanligtvis leverantören i grossistledet inte har något direkt kontraktsförhållande med slutanvändaren.

(19) Direktiv 95/46/EG fastställer en allmän ram för skydd av personuppgifter i Europeiska unionen. Kommissionen har lagt fram ett förslag till Europaparlamentets och rådets förordning som ska ersätta direktiv 95/46/EG (förordningen om dataskydd). Genom den föreslagna förordningen om dataskydd skulle det införas en skyldighet för alla registeransvariga att anmäla personuppgiftsbrott, med artikel 4.3 i direktiv 2002/58/EG som underlag. Dagens kommissionsförordning är helt och hållet förenlig med denna åtgärd.

(20) Den föreslagna förordningen om dataskydd innehåller också ett begränsat antal tekniska justeringar av direktiv 2002/58/EG för att ta hänsyn till att direktiv 95/46/EG omvandlas till en förordning. Den nya förordningens materiella rättsliga konsekvenser för direktiv 2002/58/EG kommer att granskas av kommissionen.

(21) Tillämpningen av denna förordning bör ses över tre år efter det att den träder i kraft, och dess innehåll ses över mot bakgrund av det rättsliga ramverk som gäller vid den tidpunkten, inklusive den föreslagna förordningen om dataskydd. Översynen av denna förordning bör om det är möjligt kopplas till eventuella kommande översyner av direktiv 2002/58/EG.

(22) Tillämpningen av denna förordning kan bedömas på grundval av bland annat statistik från behöriga nationella myndigheter om de personuppgiftsbrott som anmäls till dem. Sådan statistik kan bland annat omfatta uppgifter om antal personuppgiftsbrott som anmälts till den behöriga nationella myndigheten, antal personuppgiftsbrott som anmälts till abonnenter eller enskilda personer, den tid som det tagit att åtgärda personuppgiftsbrottet och huruvida tekniska skyddsåtgärder vidtagits. Genom denna statistik bör kommissionen och medlemsstaterna få enhetliga och jämförbara statistiska uppgifter. Uppgifterna ska varken avslöja identiteten på den leverantör som gör anmälan eller på inblandade abonnenter eller enskilda personer. Kommissionen kan också genomföra regelbundna möten med behöriga nationella myndigheter och andra berörda intressenter.

(23) De åtgärder som föreskrivs i denna förordning är förenliga med yttrandet från kommunikationskommittén.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Tillämpningsområde

Denna förordning ska tillämpas på anmälningar av personuppgiftsbrott som görs av leverantörer av allmänt tillgängliga elektroniska kommunikationstjänster (nedan kallad *leverantören*).

Artikel 2

Anmälan till den behöriga nationella myndigheten

1. Leverantören ska anmäla alla personuppgiftsbrott till den behöriga nationella myndigheten.

2. Leverantören ska anmäla personuppgiftsbrottet till den behöriga nationella myndigheten senast 24 timmar efter att personuppgiftsbrottet upptäckts, där så är möjligt.

Leverantören ska i sin anmälan till den behöriga nationella myndigheten inkludera de uppgifter som anges i bilaga I.

Personuppgiftsbrott ska anses ha upptäckts om leverantören har varit tillräckligt medveten om att en säkerhetsincident har inträffat som ledde till att personuppgifter äventyrats, för att göra en anmälan i enlighet med denna förordning.

3. Om inte alla uppgifter som anges i bilaga I finns tillgängliga och ytterligare utredning av personuppgiftsbrottet krävs ska leverantören ha rätt att göra en inledande anmälan till den behöriga myndigheten senast 24 timmar efter att personuppgiftsbrottet upptäckts. Denna inledande anmälan till den behöriga nationella myndigheten ska innehålla de uppgifter som anges i avsnitt 1 i bilaga I. Leverantören bör göra en andra anmälan till den behöriga nationella myndigheten så snart som möjligt och inom tre dagar från den inledande anmälan. Denna andra anmälan bör innehålla de uppgifter som anges i avsnitt 2 i bilaga I och, om det är nödvändigt, en uppdatering av redan lämnade uppgifter.

Om leverantören, trots sin utredning, inte kan tillhandahålla alla uppgifter inom tre dagar från den ursprungliga anmälan ska leverantören lämna så många uppgifter som den förfogar över inom den tidsfristen och till den behöriga myndigheten lämna en välgrundad motivering till den sena anmälan av de återstående uppgifterna. Leverantören ska snarast möjligt lämna de återstående uppgifterna till den behöriga myndigheten och, om det är nödvändigt, snarast möjligt uppdatera redan lämnade uppgifter.

4. Den behöriga nationella myndigheten ska för alla leverantörer som är etablerade i den berörda medlemsstaten tillhandahålla ett säkert sätt att på elektronisk väg anmäla personuppgiftsbrott samt information om förfarandena för åtkomst och användning. Om det är nödvändigt ska kommissionen sammankalla möten med behöriga nationella myndigheter för att underlätta tillämpningen av denna bestämmelse.

5. När personuppgiftsbrott påverkar abonnenter och enskilda personer från andra medlemsstater än den medlemsstat där personuppgiftsbrottet anmälts till den behöriga nationella myndigheten, ska den behöriga nationella myndigheten underrätta de andra nationella myndigheter som berörs.

För att underlätta tillämpningen av denna bestämmelse, ska kommissionen upprätta en förteckning över de behöriga nationella myndigheterna och lämpliga kontaktpunkter samt hålla den aktuell.

Artikel 3

Anmälan till abonnent eller enskild person

1. Om personuppgiftsbrottet kan antas inverka menligt på en abonnents eller en enskild persons personuppgifter eller integritet ska leverantören, utöver anmälan enligt artikel 2, också underrätta abonnenten eller den enskilda personen om personuppgiftsbrottet.

2. När det ska fastställas om ett personuppgiftsbrott kan antas inverka menligt på en abonnents eller enskild persons personuppgifter eller integritet ska i synnerhet följande omständigheter beaktas:

a) De berörda personuppgifternas art och innehåll, i synnerhet när de avser finansiell information, särskilda kategorier av uppgifter enligt artikel 8.1 i direktiv 95/46/EG samt lokaliseringsdata, internetloggar, webbläsarhistorik, uppgifter om e-post och specificerade samtalslistor.

b) Personuppgiftsbrottets troliga konsekvenser för den berörda abonnenten eller enskilda personen, i synnerhet om brottet skulle kunna medföra identitetsstöld eller bedrägeri, fysisk skada, psykiska men, förödmjukelse eller skadat rykte.

c) Omständigheterna för personuppgiftsbrottet, i synnerhet om uppgifterna har stulits eller om leverantören vet att uppgifterna finns hos en obehörig tredje part.

3. Anmälan till abonnenten eller den enskilda personen ska göras utan onödigt dröjsmål efter att personuppgiftsbrottet avslöjats i enlighet med artikel 2.2 tredje stycket. Detta ska inte vara beroende av den anmälan av personuppgiftsbrottet till den behöriga nationella myndighet som avses i artikel 2.

4. Leverantören ska i sin anmälan till den behöriga nationella myndigheten inkludera de uppgifter som anges i bilaga II. Anmälan till abonnenten eller den enskilda personen ska formuleras tydligt och lättbegripligt. Leverantören ska inte utnyttja anmälan som en möjlighet att marknadsföra eller annonsera om nya eller kompletterande tjänster.

5. I exceptionella fall, om anmälan till abonnenten eller den enskilda personen kan äventyra en korrekt utredning av personuppgiftsbrottet, ska leverantören ha rätt att, efter godkännande av den behöriga nationella myndigheten, skjuta upp anmälan till abonnenten eller den enskilda personen tills den behöriga nationella myndigheten anser att det är möjligt att anmäla personuppgiftsbrottet i enlighet med denna artikel.

6. Leverantören ska till abonnenten eller den enskilda personen anmäla personuppgiftsbrottet genom kommunikation som säkerställer att informationen snabbt kan mottas och som på lämpligt sätt är säkrad enligt den senaste tekniken. Informationen om personuppgiftsbrottet ska enbart omfatta uppgifter om detta brott och inte innehålla uppgifter om något annat ämne.

7. Om den leverantör som har ett direkt kontraktsförhållande med slutanvändaren, trots rimliga ansträngningar inte inom den tidsfrist som anges i punkt 3 kan identifiera alla enskilda personer på vilka personuppgiftsbrottet kan tänkas inverka menligt, får leverantören underrätta dessa enskilda personer genom annonser i större nationella eller regionala medier i de relevanta medlemsstaterna inom den tidsfristen. Dessa annonser ska innehålla de uppgifter som anges i bilaga II, om nödvändigt i förkortad form. I sådana fall ska leverantören fortsätta att göra alla rimliga ansträngningar för att identifiera dessa enskilda personer och snarast möjligt meddela dem de uppgifter som anges i bilaga II.

Artikel 4

Tekniska skyddsåtgärder

1. Med avvikelse från artikel 3.1 ska det inte vara ett krav att anmäla personuppgiftsbrottet till den berörda abonnenten eller enskilda personen om leverantören på ett tillfredsställande sätt har visat den behöriga nationella myndigheten att den har vidtagit lämpliga tekniska skyddsåtgärder och att dessa åtgärder tillämpats på de uppgifter som berördes av säkerhetsöverträdelsen. Sådana tekniska skyddsåtgärder ska göra data oläsbara för alla personer som inte är behöriga att få tillgång till uppgifterna.

2. Data ska anses oläsbara om

a) de har krypterats säkert med en standardiserad algoritm, den nyckel som används för att dekryptera data inte har äventyrats genom någon säkerhetsöverträdelse och den nyckel som används för att dekryptera data har genererats på ett sådant sätt att den inte kan utrönas med tillgängliga tekniska metoder av en person som är obehörig att använda nyckeln, eller

b) de har ersatts med sina hashvärden beräknade med en standardiserad kryptografisk hashfunktion med nyckel, den nyckel som används för kondensat av data har inte äventyrats genom någon säkerhetsöverträdelse och den nyckel som används för kondenseringen har genererats så att den inte kan utrönas med tillgängliga tekniska metoder av en person som är obehörig att använda nyckeln.

3. Kommissionen får efter samråd med de behöriga nationella myndigheterna via artikel 29-gruppen, Europeiska byrån för nät- och informationssäkerhet och Europeiska datatillsynsmannen offentliggöra en vägledande förteckning över lämpliga tekniska skyddsåtgärder enligt punkt 1, i enlighet med rådande praxis.

Artikel 5

Användning av en annan leverantör

Om en annan leverantör har kontrakterats för att leverera en del av de elektroniska kommunikationstjänsterna utan att ha ett direkt kontraktsförhållande med abonnenter ska denna andra leverantör omedelbart informera den leverantör som har tillhandahållit kontraktet i händelse av personuppgiftsbrott.

Artikel 6

Rapportering och översyn

Inom tre år efter ikraftträdandet av denna förordning ska kommissionen lägga fram en rapport om tillämpningen av denna förordning, hur effektiv den varit samt hur den påverkat leverantörer, abonnenter och enskilda personer. Med den rapporten som underlag ska kommissionen se över denna förordning.

Artikel 7

Ikraftträdande

Denna förordning träder i kraft den 25 augusti 2013.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 24 juni 2013.

På kommissionens vägnar
José Manuel BARROSO
Ordförande

BILAGA I

Innehåll i anmälan till den behöriga nationella myndigheten

Avsnitt 1

Identifiering av leverantören

1. Leverantörens namn.

2. Identitet och kontaktuppgifter för uppgiftsskyddsombudet eller andra kontaktpunkter där mer information kan erhållas.

3. Om det rör sig om en första eller andra anmälan.

Inledande uppgifter om personuppgiftsbrottet (att kompletteras i senare anmälningar, i tillämpliga fall)

4. Datum och tid för incidenten (om de är kända, i andra fall kan en uppskattning göras), samt för upptäckten av incidenten.

5. Omständigheterna kring personuppgiftsbrottet (t.ex. förlust, stöld, kopiering).

6. De berörda personuppgifternas art och innehåll.

7. Tekniska och organisatoriska åtgärder som vidtagits (eller som ska vidtas) av leverantören vad gäller personuppgifter som berörs.

8. Relevant användning av andra leverantörer (i förekommande fall).

Avsnitt 2

Kompletterande uppgifter om personuppgiftsbrottet

9. Sammanfattning av den incident som orsakade personuppgiftsbrottet (inklusive den fysiska platsen för brottet och det lagringsmedium som användes).

10. Antal berörda abonnenter eller enskilda personer.

11. Potentiella konsekvenser och potentiell menlig inverkan för abonnenter och enskilda personer.

12. Tekniska och organisatoriska åtgärder som vidtagits av leverantören för att mildra potentiell menlig inverkan.

Eventuella ytterligare anmälningar till abonnenter eller enskilda personer

13. Underrättelsens innehåll.

14. Kommunikationssätt.

15. Antal abonnenter eller enskilda personer som underrättats.

Eventuella gränsöverskridande frågor

16. Personuppgiftsbrottet berör abonnenter eller enskilda personer i andra medlemsstater.

17. Anmälan av andra behöriga nationella myndigheter.

BILAGA II

Innehåll i anmälan till abonnent eller enskild person

1. Leverantörens namn.

2. Identitet och kontaktuppgifter för personuppgiftsombudet eller andra kontaktpunkter där mer information kan erhållas.

3. Sammanfattning av den incident som orsakade personuppgiftsbrottet.

4. Uppskattat datum för incidenten.

5. De berörda personuppgifternas art och innehåll enligt artikel 3.2.

6. Förmodade konsekvenser av personuppgiftsbrottet för den berörda abonnenten eller enskilda personen enligt artikel 3.2.

7. Omständigheterna kring personuppgiftsbrottet enligt artikel 3.2.

8. Åtgärder som leverantören vidtagit för att åtgärda personuppgiftsbrottet.

9. Åtgärder som leverantören rekommenderar för att mildra den tänkbara menliga inverkan.