

Bekendtgørelse om persondatasikkerhed i forbindelse med udbud af elektroniske kommunikationsnet og -tjenester¹

I medfør af § 8, stk. 1, 2 og 4, jf. § 20, stk. 1, § 80 samt § 81, stk. 2 og 4, i lov nr. 169 af 3. marts 2011 om elektroniske kommunikationsnet og -tjenester fastsættes efter bemyndigelse i henhold til § 66, stk. 1, jf. §§ 3 og 4 i bekendtgørelse nr. [xxx af xx. xxxx 2013] om rammerne for persondatabeskyttelse i forbindelse med udbud af elektroniske kommunikationsnet og -tjenester:

Formål og anvendelsesområde

§ 1. Bekendtgørelsen har til formål at sikre persondatasikkerheden i forbindelse med udbud af offentlige elektroniske kommunikationsnet og -tjenester.

Definitioner

§ 2. I denne bekendtgørelse forstås ved:

1) *Persondatasikkerhed*:

a) Tilgængelighed: At net, tjenester og data er tilgængelige og anvendelige.

b) Fortrolighed: At data i forbindelse med net- og tjenesteudbuddet kun er tilgængelige for og kun behandles af henholdsvis fysiske eller juridiske personer, som data er tiltænkt, eller som er autoriserede hertil i henhold til lovlige formål.

c) Integritet: At data i forbindelse med net- og tjenesteudbuddet ikke forvanskes ved uautoriserede og/eller utilsigtede ændringer.

2) *Brud på persondatasikkerheden*: Sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af en offentlig elektronisk kommunikationstjeneste.

3) *Tjenesteudbyder*: Udbyder af offentlige elektroniske kommunikationstjenester.

Stk. 2. I det omfang denne bekendtgørelse refererer til begreber, som er defineret i lov om elektroniske kommunikationsnet og -tjenester og lov om behandling af personoplysninger, henvises til de i disse love fastlagte definitioner.

Risikostyring

§ 3. Tjenesteudbydere skal løbende som led i virksomhedens planlægnings- og driftsopgaver træffe passende tekniske og organisatoriske foranstaltninger med henblik på at styre risici for persondatasikkerheden i net og tjenester. Udbyderne skal sikre et sikkerhedsniveau, der, under hensyn til teknologiens aktuelle stade, står i forhold til risici.

Stk. 2. Tjenesteudbydere kan ikke overdrage ansvaret for persondatasikkerheden til tredjemand. Hvis opgaven med planlægning af persondatasikkerhed eller centrale dele af virksomhedens drifts- og/eller planlægningsopgaver i øvrigt udføres af tredjemand, skal udbyder gennem aftale og ved kontrol påse persondatasikkerheden.

§ 4. Tjenesteudbydere skal varetage persondatasikkerheden på baggrund af en dokumenteret risikostyringsproces. Udbyderne skal i den forbindelse kortlægge risici og herudfra identificere, udvælge og prioritere foranstaltninger til beskyttelse af net, tjenester og data inden for eget forretningsområde.

§ 5. Tjenesteudbydere udarbejder en sikkerhedspolitik for persondatasikkerheden i forbindelse med tjenesteudbuddet og i relevant omfang sikringsplaner, der beskriver de foranstaltninger, der iværksættes for at håndtere risici, jf. § 3 og § 4. Sådanne foranstaltninger skal, udover hvad der følger af krav til selve behandlingen af persondata i kapitel 4 i bekendtgørelse om udbud af elektroniske kommunikationsnet og -tjenester, som minimum:

1) Sikre at kun autoriserede personer får adgang til persondata til lovlige formål.

2) Beskytte lagrede persondata og persondata under transmission mod hændelig eller ulovlig tilintetgørelse, hændeligt tab eller ændring og ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse.

Særlig risiko for brud på persondatasikkerheden

§ 6. Tjenesteudbydere skal, hvor der er særlig risiko for brud på persondatasikkerheden informere slutbrugerne herom. Hvis risikoen ligger uden for de foranstaltninger, der skal træffes af udbyderen efter denne bekendtgørelse, skal der tillige informeres om, hvordan hændelsen i givet fald kan forebygges, herunder med angivelse af de omkostninger, der sandsynligvis vil være forbundet hermed.

Underretning om brud

§ 7. Underretning om brud på persondatasikkerheden efter direktiv 2002/58/EF om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor, som ændret ved direktiv 2009/136/EF, artikel 4, stk. 3, samt efter Kommissionens Forordning (EU) Nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden, jf. direktiv 2002/58/EF vedrørende databeskyttelse inden for elektronisk kommunikation, artikel 2, skal ske til Erhvervsstyrelsen.

Stk. 2. Uden at det berører tjenesteudbyders forpligtelse til underretning efter det i stk. 1 nævnte direktiv, kan Erhvervsstyrelsen i tilfælde, hvor underretning ikke allerede er sket, efter at have vurderet bruddets sandsynlige negative virkninger, kræve, at udbyder foretager underretning af slutbrugeren eller den fysiske person om sikkerhedsbruddet.

Optegnelser over brud på persondatasikkerheden

§ 8. Tjenesteudbydere skal føre optegnelser over brud på persondatasikkerheden, som indeholder oplysninger om omstændighederne vedrørende bruddene, deres virkninger og de afhjælpende foranstaltninger, der er truffet. Disse optegnelser skal være tilstrækkeligt detaljerede til, at Erhvervsstyrelsen kan føre kontrol med overholdelsen af § 7. Optegnelserne skal kun indeholde de oplysninger, der er nødvendige til dette formål.

Stk. 2. Optegnelser i henhold til stk. 1 skal opbevares i minimum 3 år.

Tests og øvelser m.v.

§ 9. Tjenesteudbydere skal løbende vurdere behovet for og foretage de nødvendige test og den nødvendige opdatering og udvikling af foranstaltninger som er iværksat og i relevant omfang beskrevet i sikringsplaner og gennemført i henhold til § 4 og § 5.

Straffebestemmelser

§ 10. Med bøde straffes den, der overtræder §§ 3-9.

Stk. 2. Der kan pålægges selskaber m.v. (juridiske personer) strafansvar efter reglerne i straffelovens 5. kapitel.

Ikrafttræden

§ 11. Bekendtgørelsen træder i kraft den 25. august 2013.

Stk. 2. Bekendtgørelse nr. 445 af 11. maj 2011 om persondatasikkerhed og beredskab for elektroniske kommunikationsnet og -tjenester ophæves².

Erhvervsstyrelsen, den xx. xxx 2013

Betina Hagerup

/ Brian Adrian Wessel

¹ Bekendtgørelsen indeholder regler, der gennemfører dele af Europa-Parlamentets og Rådets direktiv 2002/21/EF af 7. marts 2002, EF-Tidende 2002, nr. L 108, side 33, Europa-Parlamentets og Rådets direktiv 2002/22/EF af 7. marts 2002, EF-Tidende 2002, nr. L 108, side 51, Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002, EF-Tidende 2002, L 201, side 37, Europa-Parlamentets og Rådets direktiv 2009/140/EF af 25. november 2009, EF-Tidende 2009, L 337, side 37, Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009, EF-Tidende 2009, nr. L 337, side 11 og Kommissionens Forordning (EU) Nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden, jf. direktiv 2002/58/EF vedrørende databeskyttelse inden for elektronisk kommunikation, EF-Tidende 2013, nr. L 173, side 2.

² Ophævelsen af bekendtgørelsen sker på baggrund af den kongelige resolution af 3. oktober 2011, hvor ressortansvaret for tele- og internetregulering samt administration af frekvenser blev overført til Erhvervs- og Vækstministeriet og ressortansvaret for sager vedrørende beskyttelse af kritisk it-infrastruktur, samt statens varslings-tjeneste for internettrusler, GovCert, blev overført til Forsvarsministeriet.