VEJLEDNING

6. februar 2017
Revideret 24. maj 2018

Vejledning til bekendtgørelse om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester

ERHVERVSSTYRELSEN
Dahlerups Pakhus
Langelinie Allé 17
2100 København Ø

Tlf. 35 29 10 00
Fax 35 29 10 01
CVR-nr 10 15 08 17
E-post erst@erst.dk
www.erst.dk

ERHVERVS- OG VÆKSTMINISTERIET

Indholdsfortegnelse

1. Indledning

Denne vejledning beskriver og uddyber de krav, der følger af bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester (i det følgende omtalt som "bekendtgørelsen"). Bekendtgørelsen trådte i kraft den 1. juli 2016.

Bekendtgørelsens regler er ikke nye. Siden 2011 har der været særlige regler om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester. Det oprindelige regelsæt[1] havde imidlertid et mere omfattende indhold. Bl.a. regulerede det generelt informationssikkerhed (ikke kun persondatasikkerhed), og det indeholdt også regler om beredskab for elektroniske kommunikationsnet og -tjenester.

Ansvaret for de oprindelige regler blev i forbindelse med en ressortændring i 2011 delt mellem to ministerier – Forsvarsministeriet og Erhvervs- og Vækstministeriet. Det affødte et behov for at dele reglerne op. Denne opdeling er bl.a. resulteret i følgende regler, der trådte i kraft den 1. juli 2016:

Bekendtgørelsens titel	**Udstedt af**
Bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester	Erhvervs- og vækstministeren
Bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester	Center for Cybersikkerhed (under Forsvarsministeriet)
Bekendtgørelse nr. 566 af 1. juni 2016 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed	Center for Cybersikkerhed

Forholdet mellem de forskellige regelsæt beskrives nærmere nedenfor i afsnit 2.4 og 5.2.2.

Bekendtgørelsen har baggrund i direktiv 2002/58/EF, som også kaldes e-databeskyttelsesdirektivet (eller e-privacy-direktivet). E-databeskyttelses-direktivet supplerer de generelle EU-regler om beskyttelse af persondata og fastsætter særlige regler om databeskyttelse og privatlivsbeskyttelse på området for elektronisk kommunikation.

[1] Bekendtgørelse nr. 396 af 21. april 2011 om rammerne for informationssikkerhed og beredskab og bekendtgørelse nr. 445 af 11. maj 2011 med senere ændringer.

2. Bekendtgørelsens anvendelsesområde - Bekendtgørelsens § 1

2.1. Hvem er forpligtet i henhold til bekendtgørelsens regler?
Bekendtgørelsens regler gælder for udbydere af offentlige elektroniske kommunikationstjenester – det vil sige elektroniske kommunikationstjenester, der stilles til rådighed for en ikke på forhånd afgrænset kreds af slutbrugere eller udbydere af elektroniske kommunikationsnet eller -tjenester. Det er fx udbydere af telefoni- og internettjenester, uanset om den pågældende tjeneste udbydes via fastnet eller mobilnet.

Udbyderbegrebet er defineret i telelovens[2] § 2, nr. 1. Heraf fremgår, at en udbyder er den, som med kommercielt formål stiller produkter, elektroniske kommunikationsnet eller tjenester omfattet af denne lov til rådighed for andre.

Det kommercielle grundlag foreligger, såfremt der er tale om en aktivitet, som tilbydes eller efterspørges på markedsmæssige vilkår, herunder hvis aktiviteten er af generel karakter og rettet til en modtagerkreds, som kan forventes at betale herfor.

Det er uden betydning, om de pågældende har anlagt egen infrastruktur eller baserer deres aktiviteter fuldt ud på lejet infrastrukturkapacitet.

Energistyrelsen har udarbejdet yderligere vejledning, der præciserer, hvem der er omfattet af udbyderbegrebet, se under punkterne "Hvornår er man udbyder" og "Generel vejledning om udbyderbegrebet" på dette link

2.2. Hvilke persondata er omfattet af bekendtgørelsen?
Personoplysninger defineres i databeskyttelsesforordningen (GDPR) [3] som enhver form for information om en identificeret eller identificerbar fysisk person. Bekendtgørelsen omfatter *persondata, som behandles i forbindelse med et udbud af offentlige elektroniske kommunikationstjenester*. Det omfatter eksempelvis kunders cpr-numre, regningsoplysninger, opkaldslister, trafikdata, indholdet af sms-beskeder og telefonsamtaler osv.

2.3. Forholdet til de generelle regler om beskyttelse af persondata
Databeskyttelsesforordningen (GDPR) indeholder de generelle regler om beskyttelse af persondata. Forordningen indeholder regler om behandling af personoplysninger, om registreredes rettigheder, behandlingssikkerhed m.m. og gælder på tværs af offentlige og private sektorer. Databeskyttelsesloven[4] indeholder regler, der supplerer databeskyttelsesforordningen. Det er Datatilsynet, der er tilsynsmyndighed i forhold til forordningen og databeskyttelsesloven.

---

[2] Lov om elektroniske kommunikationsnet og -tjenester, jf. lovbekendtgørelse nr. 128 af 7. februar 2014 med senere ændringer.
[3] Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF.
[4] Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger.

Reglerne om behandling af personoplysninger i den elektroniske kommunikationssektor[5] er såkaldt sektorspecifikke regler, der specificerer og supplerer de generelle regler om beskyttelse af personoplysninger.

Udbydere af elektroniske kommunikationstjenester, der er omfattet af bekendtgørelsen om persondatasikkerhed i forbindelse med udbud af elektroniske kommunikationstjenester, skal således være opmærksomme på, at der er regler i den generelle persondatalovgivning, som de også skal følge. Det gælder fx udbydernes behandling af persondata, der vedrører deres medarbejdere, eller udbydernes pligt til at give deres kunder indsigt i de data, udbyderne har registeret om kunden.

2.4. Forholdet til reglerne om informationssikkerhed

Lov om net- og informationssikkerhed[6], der administreres af Center for Cybersikkerhed, indeholder hjemmel for Center for Cybersikkerhed til at fastsætte regler om minimumskrav til informationssikkerhed for udbydere af offentligt tilgængelige net og tjenester[7]. I medfør heraf er der bl.a. fastsat regler om, at udbydere af offentlige elektroniske kommunikationsnet og -tjenester på baggrund af en risikovurdering skal implementere passende foranstaltninger til sikring af tilgængelighed, integritet og fortrolighed i net og tjenester samt sikre, at tredjepart opretholder en tilsvarende sikkerhed i forhold til driftsleverancer til udbyderne.[8]

I medfør af lov om net- og informationssikkerhed har Center for Cybersikkerhed endvidere fastsat regler om underretning til Center for Cybersikkerhed om brud på informationssikkerheden[9].

Afsnit 5.2.2 behandler grænsefladen mellem Center for Cybersikkerheds krav til underretning om brud på informationssikkerheden og bekendtgørelsens regler om underretning til Erhvervsstyrelsen om brud på persondatasikkerheden.

Reglerne om net- og informationssikkerhed vedrører tilgængelighed, integritet og fortrolighed i offentligt tilgængelige net og tjenester, mens bekendtgørelsen alene vedrører persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester. Som det også er beskrevet i afsnit 5.2.2 kan der være situationer, hvor begge regelsæt skal iagttages, fx fordi en hændelse både kan udgøre et brud på persondatasikkerheden og et brud på informationssikkerheden. Tilsvarende kan en given sikkerhedsforanstaltning være relevant for såvel informations- som persondatasikkerheden. Men der er også situationer, som kun er omfattet af enten det ene eller det andet regelsæt.

---

[5] Herunder bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

[6] Lov nr. 1567 af 15. december 2015.

[7] Definitionen af "offentligt tilgængelige net og tjenester", der anvendes i lov om net- og informationssikkerhed samt bekendtgørelser udstedt i medfør heraf, svarer til definitionen af såvel "offentlige elektroniske kommunikationsnet" i telelovens § 2, nr. 5, som "offentlige elektroniske kommunikationstjenester" i telelovens § 2, nr. 8.

[8] Jf. bekendtgørelse nr. 567 af 1. juni 2016 om informationssikkerhed og beredskab i net og tjenester.

[9] Jf. bekendtgørelse nr. 566 af 1. juni 2016 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

Erhvervsstyrelsen og Center for Cybersikkerhed koordinerer løbende deres arbejde med de to regelsæt og vejleder udbydere om reglerne og deres anvendelsesområde.

2.5. Andre sektorspecifikke regler på teleområdet om behandling af persondata

Telelovgivningen indeholder også andre sektorspecifikke regler af relevans for behandling af persondata på teleområdet, herunder særligt §§ 20-24 i bekendtgørelse om udbud af elektroniske kommunikationsnet og -tjenester[10] om fx behandling af trafik- og lokaliseringsdata samt telelovens § 7 om hemmeligholdelse af oplysninger i forbindelse med udbud af elektroniske kommunikationsnet og -tjenester.

3. Risikostyring – Bekendtgørelsens § 3

Bekendtgørelsen er grundlæggende udtryk for en videreførelse af tidligere gældende regulering vedrørende persondatabeskyttelse på teleområdet. De forskelle, der er mellem de gamle og de nye regler har således ikke betydning for de forpligtelser, udbydere af offentlige elektroniske kommunikationstjenester har til at beskytte persondata i forbindelse med udbud af offentlige elektroniske kommunikationstjenester. Kravene til sikkerhedsniveauet er uændret, men den ny bekendtgørelse indebærer, at de omfattede udbydere har øget fleksibilitet til at leve op til kravene.

Efter bekendtgørelsens § 3 skal udbydere af offentlige elektroniske kommunikationstjenester løbende *træffe passende tekniske og organisatoriske foranstaltninger* med henblik på at styre risici for persondatasikkerheden i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

Det fremgår specifikt af bekendtgørelsens § 3, stk. 2, at de foranstaltninger, der skal træffes, som minimum skal

1) sikre, at kun autoriserede personer får adgang til persondata til lovlige formål,
2) beskytte lagrede eller sendte persondata mod hændelig eller ulovlig tilintetgørelse, hændeligt tab eller ændring og ubeføjet eller ulovlig lagring, behandling, adgang eller videregivelse, og
3) gennemføre en sikkerhedspolitik for persondatasikkerheden i forbindelse med udbud af elektroniske kommunikationstjenester.

Pligten til at træffe passende foranstaltninger som nævnt i bestemmelsen påhviler *udbydere af offentlige elektroniske kommunikationstjenester*. Hvis det er nødvendigt for at leve op til de forpligtelser, der følger af bekendtgørelsen, må udbyderen af den offentlige elektroniske kommunikationstjeneste samarbejde med den udbyder, der leverer det underliggende elektroniske kommunikationsnet (infrastrukturen).

3.1. Hvad kan "passende" foranstaltninger være?

De foranstaltninger, der skal træffes, skal *sikre et sikkerhedsniveau, der under hensyn til teknologiens aktuelle stade og omkostningerne i forbindelse med gennemførelsen af foranstaltningerne, står i forhold til risici"*[11]. En "passende"

[10] Bekendtgørelse nr. 715 af 23. juni 2011.
[11] Jf. bekendtgørelsens § 3, stk. 1, 2. pkt.

foranstaltning er altså en foranstaltning, der er proportional i forhold til de risici, som den skal sikre imod under hensyntagen til den teknologiske udvikling.

Det er ikke krav, at man har implementeret de nyeste og bedste sikkerhedsteknologier til beskyttelse af persondata, men man skal løbende evaluere og revurdere sine sikkerhedsforanstaltninger i takt med den teknologiske udvikling.

Det er op til den enkelte udbyder af offentlige elektroniske kommunikationstjenester at beslutte, hvordan man konkret vil indrette sig for at leve op til bekendtgørelsens krav. Den internationale standard ISO27001 om informationssikkerhed giver en generelt dækkende vejledning om etablering af såvel tekniske som organisatoriske sikkerhedsforanstaltninger, der også dækker det område, bekendtgørelsen regulerer. Det er *ikke* et krav, at man skal være certificeret efter ISO27001-standarden eller tilsvarende standarder, men det kan være en god idé at følge principperne i denne eller tilsvarende standarder for it-sikkerhed.

Derudover kan der hentes *inspiration* i bekendtgørelse om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning (sikkerhedsbekendtgørelsen)[12] og Datatilsynets tilhørende vejledning[13]. Sikkerhedsbekendtgørelsen stiller krav om organisering, fysisk sikring, administration af autorisation og adgangskontrol, behandling og destruktion af ind- og uddatamateriale og medier, awareness, mobile arbejdspladser og logning.

Sikkerhedsbekendtgørelsen, der formelt set kun gælder for behandling af persondata, der foretages for den offentlige forvaltning, er udstedt med hjemmel i persondataloven og udmønter således regler i den generelle persondatalovgivning. Men persondatalovens regler om behandlingssikkerhed minder meget om telelovgivningens sektorspecifikke regler om samme emne.

Kravet om at træffe "passende foranstaltninger" indebærer, at man tilrettelægger og organiserer sine sikkerhedsforanstaltninger, så de er tilpasset karakteren af de persondata, der er tale om, og den skade, der kan opstå, hvis der sker et brud på sikkerheden. Hvis data fx opbevares i krypteret form, er risikoen for indsigt i personlige forhold reduceret, og eventuelle foranstaltninger tager i den situation udgangspunkt i en vurdering af risikoen for, at uvedkommende kan dekryptere data.

For at kunne beslutte, hvilke foranstaltninger det konkret er nødvendigt at gennemføre, kan det være hensigtsmæssigt at foretage en *risikovurdering* med udgangspunkt i følgende:

- Skab et overblik over de persondata, man har, og som man behandler i forbindelse med udbuddet af offentlige elektroniske kommunikationstjenester.
- Hvad er de potentielle trusler? Hvordan ser risikobilledet ud?
- Karakteren og omfanget af organisationens lokaliteter og it-systemer.
- I hvilken grad medarbejderne har adgang til persondata.
- Hvilke persondata, der behandles af tredjeparter på ens vegne.

[12] Justitsministeriets bekendtgørelse nr. 528 af 15. juni 2000 med senere ændringer.
[13] Vejledning nr. 37 af 2. april 2001.

De sikkerhedsforanstaltninger, det kan være relevant at træffe på baggrund af risikovurderingen, kan groft sagt opdeles i:

1) Ledelsesmæssige og organisatoriske foranstaltninger.
2) Foranstaltninger i forhold til medarbejdere.
3) Foranstaltninger i forhold til tredjeparters behandling af data.
4) Foranstaltninger i forhold til adgang til systemer.
5) Foranstaltninger i forhold til fysisk sikkerhed.
6) Foranstaltninger i forhold til it-systemers sikkerhed.

Som nævnt i afsnit 2.4 er der i medfør af lov om net- og informationssikkerhed, der administreres af Center for Cybersikkerhed, fastsat regler om, at udbydere af offentlige elektroniske kommunikationsnet og -tjenester på baggrund af en risikovurdering skal implementere passende foranstaltninger til sikring af tilgængelighed, integritet og fortrolighed i net og tjenester samt sikre, at tredjepart opretholder en tilsvarende sikkerhed i forhold til driftsleverancer til udbyderne. De foranstaltninger, der skal gennemføres for at efterleve disse regler, vil i et vist omfang være sammenfaldende med de foranstaltninger, der efter bekendtgørelsen skal træffes for at styre risici for persondatasikkerheden. For udbydere, der er omfattet af reglerne om net- og informationssikkerhed, vil det derfor være relevant at sammentænke implementeringen af de krav, der stilles efter de to regelsæt.

3.1.1. Ledelsesmæssige og organisatoriske foranstaltninger

Det er vigtigt at have klarhed over, hvem der i ens organisation er *ansvarlig for sikkerheden* i forbindelse med beskyttelse af persondata. Fx kan det være en god idé at udpege en person eller en afdeling i organisationen som dag-til-dag-ansvarlig for sikkerheden, som har den nødvendige autoritet og de nødvendige ressourcer til at varetage de opgaver, der følger med ansvaret.

En vigtig opgave i denne sammenhæng er at udarbejde en *sikkerhedspolitik*. Det fremgår direkte af bekendtgørelsen, at udbydere af offentlige elektroniske kommunikationstjenester *skal* have en sikkerhedspolitik for persondatasikkerheden i forbindelse med udbud af offentlige elektroniske kommunikationstjenester, jf. bekendtgørelsens § 3, stk. 2, nr. 3.

Bekendtgørelsen indeholder ikke specifikke krav til, hvordan sikkerhedspolitikken skal udformes, men eksempelvis har Dansk Industri udarbejdet en skabelon for en it-sikkerhedspolitik, som kan være til inspiration. Skabelonen kan findes her

For at sikre, at sikkerhedspolitikken er tidssvarende, bør den revideres løbende og opdateres ved behov.

3.1.2. Foranstaltninger i forhold til medarbejdere

Det er vigtigt, at medarbejdere, som håndterer persondata, forstår vigtigheden af at beskytte persondata, og at de er bekendt med organisationens sikkerhedspolitik. Dette kan fx sikres ved løbende at give medarbejderne relevant instruktion og uddannelse. Formålet er, at viden om sikkerhedsforanstaltninger mv. er forankret hos medarbejderne.

Fx bør medarbejderne, herunder ansatte i butikker, der handler på udbyderens vegne, være opmærksomme på risikoen for, at uvedkommende forsøger at få

adgang til en kundes persondata eller ændre oplysninger om en kundes abonnementsforhold (eksempelvis ved at udgive sig for at være den person, oplysningerne vedrører). Og ikke mindst bør de instrueres i, hvordan de forhindrer, at dette sker (fx ved at anvende særlige processer til autentifikation af kunderne).

Et andet eksempel er instruktion til medarbejdere om brug af it-udstyr med henblik på at undgå virus og lignende.

Det vil ligeledes være relevant at sikre, at medarbejdere, der har adgang til persondata, underlægges *tavshedspligt*[14].

3.1.3. Foranstaltninger i forhold til tredjeparters behandling af data

Det er altid udbyderen af offentlige elektroniske kommunikationstjenester, der har ansvaret for at beskytte de persondata, udbyderen er ansvarlig for efter de almindelige regler om persondatabeskyttelse.

Det er derfor vigtigt, at udbyderen gennem aftale sikrer, at bekendtgørelsens krav bliver overholdt, hvis udbyderen benytter sig af eksterne samarbejdsparter (tredjeparter), som har adgang til persondata, som udbyderen er ansvarlig for. Det kan eksempelvis være tilfældet ved outsourcing. Sikring kan fx ske ved, at tredjeparten bekræfter at have et sikkerhedsniveau, der lever op til bekendtgørelsens krav, samt at der indgås fortrolighedserklæringer.

3.1.4. Foranstaltninger i forhold til adgang til systemer

Det vil være en passende foranstaltning at sikre,

- at kun personer, der er godkendt til det, kan tilgå, ændre, videregive og slette persondata, og
- at de personer, der er godkendt, kun handler inden for rammerne af deres godkendelse.

Der bør derfor fastlægges procedurer for godkendelser, således at det fx er klart, hvem der har ansvaret for godkendelser, hvem der kan godkendes til hvad, hvordan det sikres, at kun personer, der er godkendt, kan få adgang til persondata, hvornår og hvordan godkendelsen skal tilbagekaldes osv.

Ovenstående indebærer bl.a.,

- at der kun gives godkendelse til medarbejdere, som beskæftiger sig med opgaver, hvor det er nødvendigt at have adgang til de pågældende persondata, og at godkendelsen begrænses til, hvad der er nødvendigt,
- at medarbejderne er orienteret om, hvilke oplysninger vedkommende er godkendt til at anvende,
- at godkendelsen inddrages, når den pågældende medarbejder ikke længere har behov for at kunne få adgang til de omhandlede persondata,

[14] Det følger af § 7 i lov om elektroniske kommunikationsnet og -tjenester, at 1) udbydere af elektroniske kommunikationsnet eller -tjenester og deres ansatte og tidligere ansatte ikke uberettiget må videregive eller udnytte oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf, som de får kendskab til i forbindelse med det pågældende udbud af elektroniske kommunikationsnet eller -tjenester, og 2) at udbyderne skal træffe de foranstaltninger, der er nødvendige for at sikre, at oplysninger om andres brug af nettet eller tjenesten eller indholdet heraf ikke er tilgængelig for uvedkommende.

- at der er teknisk adgangskontrol til de relevante systemer, således at de medarbejdere, der er godkendt, skal identificere sig over for systemet for at få adgang (fx via brugernavn og password),
- at der er retningslinjer for behandling og opbygning af password, hvis disse benyttes som adgangskontrol, herunder hvor hyppigt de skal ændres, og
- at det logges, hvem der tilgår persondata i systemerne.

Det kan også være nødvendigt at anvende principperne for godkendelse over for personer, der midlertidigt skal have adgang til persondata – fx i forbindelse med teknisk vedligeholdelse, driftsovervågning og fejlretning. I så fald er det vigtigt at sørge for, at der kun gives godkendelse til de formål og den tid, der er nødvendig.

3.1.5. Foranstaltninger i forhold til fysisk sikkerhed

Fysisk sikkerhed handler i denne sammenhæng om, at der træffes forholdsregler for at forhindre, at uvedkommende får adgang til persondata på steder, hvor sådanne data behandles. Foranstaltningerne kan bl.a. omfatte

- sikring af døre og låse,
- alarmer og overvågning,
- adgangskontrol til organisationens lokaliteter for såvel medarbejdere som gæster,
- håndtering af papiraffald,
- begrænset adgang til serverrum,
- placering af skærme og printere, og
- sikring af bærbart udstyr – fx ved hjælp af kryptering.

Under denne kategori af foranstaltninger hører også foranstaltninger i forbindelse med reparation/service og afskaffelse af udstyr, hvor der er lagret persondata. Hvis ikke oplysningerne (kan) fjernes fra udstyret, inden det gøres klar til reparation eller service, kan foranstaltningerne gå ud på at sikre, at det personale, der står for dette arbejde, behandler evt. persondata, som de måtte blive bekendt med, fortroligt og ikke videregiver data til andre, eller at lagrede oplysninger på udstyr, der skal bortskaffes, slettes, så de ikke længere kan læses.

3.1.6. Foranstaltninger i forhold til it-systemers sikkerhed

Sikkerhed i forhold til it-systemer ændrer sig hele tiden og er meget komplekst. Grundlæggende handler det om, at sikkerhedsforanstaltningerne - ud fra en afvejning også af de omkostningsmæssige aspekter - er tilpasset organisationens systemer, den teknologiske udvikling og ikke mindst de identificerede risici og trusler, jf. ovenfor.

Foranstaltninger i forhold til it-systemers sikkerhed handler bl.a. om,

- løbende at træffes foranstaltninger for at forhindre, at de it-systemer, der indeholder eller giver adgang til persondata, er udsat for angreb af skadevoldende programmer (virus m.v.),
- at træffe foranstaltninger for at sikre, at der ved brug af hjemmearbejdspladser ikke sker kompromittering af persondatasikkerheden,
- at træffe foranstaltninger, der sikrer, at persondata kan genskabes, hvis de fortabes, ændres eller ødelægges - fx ved at foretage sikkerhedskopiering (back up) efter nærmere fastlagte rutiner, og
- kryptering af fortrolige oplysninger

4. Information til brugere ved særlig risiko for brud på persondatasikkerheden – Bekendtgørelsens § 4

Hvis der er *særlig risiko* for brud på persondatasikkerheden, skal udbydere af offentlige elektroniske kommunikationstjenester informere deres slutbrugere herom, jf. bekendtgørelsens § 4.

Som det fremgår nedenfor i afsnit 5.2.3 skal udbyderne i visse tilfælde underrette slutbrugere og fysiske personer om brud på persondatasikkerheden. Til forskel herfra vedrører bestemmelsen i § 4 den situation, hvor der (endnu) ikke er sket et sikkerhedsbrud, men hvor udbyderen ved, at der er en særlig risiko herfor.

Det er særligt vigtigt, at udbyderne informerer slutbrugerne om sikkerhedsrisici, som udbyderen ikke selv har mulighed for at afhjælpe. Det fremgår således af bekendtgørelsens § 4, at hvis den særlige risiko ligger uden for de foranstaltninger, der skal træffes af udbyderen efter bekendtgørelsen, så skal udbyderen informere slutbrugerne om, hvordan hændelsen i givet fald kan forebygges, og hvilke omkostninger der sandsynligvis vil være forbundet hermed. Det betyder med andre ord, at hvis en udbyder bliver bekendt med en særlig risiko for brud på persondatasikkerheden, som kan have betydning for udbyderens kunder, men som udbyderen ikke selv kan sikre imod, så skal udbyderen informere kunderne om risikoen og om, hvad kunderne selv kan gøre for at forebygge, at deres data kompromitteres. Det kan fx dreje sig om information om risiko for virusangreb, phishing og hacking, og hvordan brugerne kan sikre deres kommunikation ved at anvende bestemte typer software (fx anti-virus og firewall-programmer), krypteringsteknologier eller ved at skifte passwords mv., der bruges til log-in, foretage sikkerhedskopiering (back up) af data, løbende opdatere styresystemer og mailprogrammer mv.

Kravet om at underrette slutbrugere om særlige sikkerhedsrisici fritager ikke udbyderne for pligten til – for egen regning – at træffe passende foranstaltninger til at forebygge nye uforudsete sikkerhedsrisici og genoprette det normale sikkerhedsniveau, jf. bekendtgørelsens § 3.

5. Underretning om brud på persondatasikkerheden – Bekendtgørelsens § 5 og EU-forordning 611/2013 af 24. juni 2013

Telesektorens underretninger om brud på persondatasikkerheden sker efter en fast procedure, som er detaljeret beskrevet i Kommissionens forordning (EU) Nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden, jf. Europa-Parlamentets og Rådets direktiv 2002/58/EF vedrørende databeskyttelse inden for elektronisk kommunikation.

5.1. Hvad er brud på persondatasikkerheden?

Ved et brud på persondatasikkerheden forstås i denne sammenhæng et 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, jf. bekendtgørelsens § 2.

Rent teknisk kan der ske et brud på persondatasikkerheden, når udbyderens system ikke er tilstrækkelig sikret, således at udefrakommende får adgang til persondata (fx hacking). Det kan imidlertid også være udbyderens egen håndtering af persondata, der kan forårsage et brud, fx hvis udbyderen ubeføjet videregiver eller ændrer persondata eller ulovligt eller hændeligt (fx brand eller oversvømmelse) tilintetgør persondata. Følgende er eksempler på brud på persondatasikkerheden:

1) Andre personer end den eller de personer hos udbyderen, der er autoriseret til det, får (uautoriseret) adgang til persondata. Det kan både være personer uden for eller inden for udbyderens organisation.
2) Udbyderens medarbejdere ændrer eller sletter persondata ved et uheld.
3) Brud på udbyderens server, hvor uvedkommende har fået indsigt i persondata - fx kundedatabasens cpr-oplysninger, kreditkortoplysninger el.lign.
4) Udbyderens medarbejdere videregiver ubevidst eller bevidst persondata om en abonnent til en anden abonnent eller anden person.
5) Når manglede kryptering af udbyderens hjemmeside indeholdende et abonnentlogin resulterer i, at en eller flere uvedkommende får direkte adgang til abonnenters persondata.

5.2. Underretningskravene

Ifølge forordningen skal udbydere af offentlige elektroniske kommunikationstjenester

1) *underrette den kompetente nationale myndighed* om samtlige brud på persondatasikkerheden (artikel 2) og
2) *underrette en abonnent eller en evt. berørt fysisk person*, hvis bruddet på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred for abonnenten eller den fysiske person (artikel 3).

5.2.1. Underretning af den kompetente nationale myndighed

Det fremgår af bekendtgørelsens § 5, stk. 1, at den underretning, der skal ske efter forordningens artikel 2, skal ske til Erhvervsstyrelsen, som således er den kompetente danske myndighed efter forordningen.

En underretning om brud på persondatasikkerheden til Erhvervsstyrelsen skal overholde den procedure, som fremgår af artikel 2 i forordningen. Proceduren indebærer bl.a. følgende:

- Underretningen skal ske senest 24 timer efter, at bruddet er påvist[15], når dette er praktisk muligt. Udbyderen skal i sin underretning af Erhvervsstyrelsen vedlægge de oplysninger, der er angivet i forordningens bilag I.

[15] Et brud på persondatasikkerheden anses for at være *påvist*, hvis en udbyder har opnået tilstrækkelig kendskab til, at en sikkerhedshændelse er indtruffet, og at den har kompromitteret persondatasikkerheden, således at der kan afgives en hensigtsmæssig underretning til myndigheden, jf. forordningens art. 2, stk. 2, 3. pkt. Efter forordningens betragtning 8 vil en simpel formodning om, at et brud på persondatasikkerheden har fundet sted, eller en simpel påvisning af en hændelse *ikke* være tilstrækkeligt, til at anse et brud på persondatasikkerheden for at være *påvist* i forordningens forstand. Bruddet er således ikke påvist, hvis de oplysninger, der er til rådighed for udbyderen,

- Udbyderen må foretage en indledende underretning senest 24 timer efter påvisning af bruddet på persondatabeskyttelsen, hvis ikke alle de oplysninger, der fremgår af forordningens bilag I, foreligger, og der er behov for yderligere efterforskning af bruddet på persondatasikkerheden. Den indledende underretning skal indeholde de oplysninger, der er anført i forordningens bilag I, afdeling 1.
- Udbyderen skal foretage en anden underretning så hurtigt som muligt og senest tre dage efter den indledende underretning. Denne anden underretning skal indeholde de oplysninger, der er anført i forordningens bilag I, afdeling 2, og om nødvendigt ajourføre de oplysninger, der allerede er afgivet.
- Hvis udbyderen på trods af sin efterforskning ikke er i stand til at forelægge alle oplysninger senest tre dage efter den indledende underretning, skal udbyderen afgive alle de oplysninger, udbyderen har til rådighed, inden for denne tidsfrist og forelægge Erhvervsstyrelsen en begrundelse for den forsinkede underretning. Udbyderen forelægger hurtigst muligt de resterende oplysninger og ajourfører om nødvendigt de oplysninger, der allerede er afgivet.

Efter forordningens artikel 2, stk. 4, skal der stilles sikre elektroniske midler til rådighed til brug for udbyderes underretning om brud på persondatasikkerheden. I Danmark er dette krav implementeret, ved at udbydere af elektroniske kommunikationstjenester via portalen Virk kan indberette brud på persondatasikkerheden til Erhvervsstyrelsen. Linket til det pågældende sted på Virk kan findes her

5.2.2.Grænseflade til Center for Cybersikkerhed

Efter § 7 i bekendtgørelse nr. 566 af 1. juni 2016 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed, som er udstedt af Center for Cybersikkerhed, skal udbydere af offentligt tilgængelige net og tjenester underrette Center for Cybersikkerhed ved brud på informationssikkerheden, der har væsentlige følger for driften af net og tjenester, jf. bekendtgørelsens § 8.

Hvis der er sket et sikkerhedsbrud, skal udbydere af offentlige elektroniske kommunikationstjenester således overveje, om underretning skal ske til Erhvervsstyrelsen, Center for Cybersikkerhed eller i visse tilfælde begge myndigheder.

Det fremgår af bemærkningerne til forslag L 10 til lov om net- og informationssikkerhed[16], at brud på informationssikkerheden omfatter tab af både tilgængelighed, integritet og fortrolighed i net og tjenester. Betingelsen om, at bruddet skal have væsentlige følger for driften af net eller tjenester, skal forstås som opretholdelse af net- eller tjenesteudbuddet.

er utilstrækkelige til at fastslå dette, selvom udbyderen gør sit bedste for at skabe afklaring. I vurderingen af om et brud er påvist, skal der tages særligt hensyn til, om de oplysninger, der er nævnt i forordningens bilag I, står til rådighed for udbyderen, fx oplysninger om omstændighederne ved bruddet på persondatasikkerheden (fx bortkomst, tyveri eller kopiering).

[16] Jf. lov nr. 1567 af 15. december 2015.

Det følger videre af lovbemærkningerne, at et brud på tilgængeligheden af net eller tjenester, som har væsentlige følger for driften af net eller tjenester, eksempelvis kan være en længerevarende afbrydelse af en udbudt tjeneste, som rammer et større geografisk område på baggrund af en overgravning af en central transmissionsforbindelse. Herudover kan brud på fortroligheden i net eller tjenester, som har væsentlige følger for driften, eksempelvis være tilfælde, hvor passwords og brugernavne og lignende følsomme informationer, som er vigtige for den centrale del af driften, bliver gjort offentligt tilgængelige eller på anden vis kompromitteres, således at udbyderen tvinges til at tage betydelige forholdsregler med henblik på at sikre nettet eller tjenesten mod angreb. Forvanskning af centrale data i forbindelse med en uberettiget adgang til net eller tjenester, således at den elektroniske kommunikation ikke overføres til de rette adressater, kan endvidere udgøre et brud på integriteten, som har væsentlige følger for driften af net eller tjenester.

Væsentlige følger for driften af net og tjenester foreligger, når følgerne overstiger de grænseværdier m.v., som følger af § 8 i bekendtgørelse nr. 566 af 1. juni 2016 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed.

Som eksempel kan nævnes, at en udbyder af mobiltelefoni skal underrette Center for Cybersikkerhed ved brud på informationssikkerheden, når bruddet har berørt over 35.000 brugere i mere end én time.

Der kan være tilfælde, hvor en hændelse udgør såvel et brud på persondatasikkerheden som et brud på informationssikkerheden. Et brud på informationssikkerheden vil således tillige være et brud på persondatasikkerheden, hvis bruddet fører til kompromittering af persondata[17]. Tilsvarende kan et brud på persondatasikkerheden samtidig være et brud på informationssikkerheden, hvis bruddet udgør en hændelse, der fx kompromitterer integriteten i net eller tjenester. I sådanne tilfælde skal der ske underretning til *såvel Erhvervsstyrelsen som Center for Cybersikkerhed*.

Som eksempel på sikkerhedsbrud, hvor der *kun skal ske underretning til Erhvervsstyrelsen*, kan nævnes:

- En medarbejder hos en udbyder udleverer persondata om en abonnent til en uvedkommende person – fx ved en fejl eller uden at sikre sig, at den pågældende er berettiget til at modtage oplysningen, fx fordi medarbejderen ikke anmoder om kundenummer el.lign.
- Fremsendelse af specificeret telefonregning til en forkert modtager.

De væsentligste forskelle på de to regelsæt om underretning om sikkerhedsbrud til hhv. Erhvervsstyrelsen og Center for Cybersikkerhed er:

- Der skal ske underretning til Erhvervsstyrelsen i alle tilfælde af brud på persondatasikkerheden i forbindelse med udbud af offentlige elektroniske kommunikationstjenester, mens kravet om underretning til Center

[17] Jf. § 2 i bekendtgørelse nr. 462 af 3. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

for Cybersikkerhed om brud på informationssikkerheden kun omfatter brud, der har væsentlige følger for driften af net og tjenester[18].
- Underretning til Erhvervsstyrelsen skal som udgangspunkt ske, senest 24 timer efter bruddet er påvist, mens underretning til Center for Cybersikkerhed skal ske, senest 14 dage efter, at det er konstateret, at bruddet har fået væsentlige følger for driften af net og tjenester.

De to underretningsprocesser er opsummeret i nedenstående skema.

Erhvervsstyrelsen	**Center for Cybersikkerhed**
Underretning til Erhvervsstyrelsen skal ske ved ethvert påvist brud på persondatasikkerheden.	Underretning til Center for Cybersikkerhed skal ske ved brud på informationssikkerheden, der har væsentlige følger for driften af net og tjenester.
Krav om et elektronisk format til underretning. ERST har etableret et underretningssystem på Virk.	Krav om skriftlig underretning. Underretningen kan sendes til teletilsyn@cfcs.dk.
Krav om afgivelse af særlige oplysninger, jf. bilag til forordningen.	Krav om afgivelse af særlige oplysninger, jf. bilag til bekendtgørelsen.
Underretningen skal efter forordningen som udgangspunkt ske senest 24 timer efter, at bruddet på persondatasikkerheden er påvist.	Underretning skal ske senest 14 dage efter, at det er konstateret, at bruddet på informationssikkerheden har fået væsentlige følger for driften af net og tjenester.

Hvis en udbyder sender en underretning til den ene af de to myndigheder, og myndigheden vurderer, at der kan være tale om et tilfælde, hvor også den anden myndighed skal underrettes, vil den første myndighed vejlede udbyderen herom.

Hvis en udbyder er i tvivl om, hvortil en underretning skal sendes, vejleder begge myndigheder selvsagt også herom.

5.2.3. Underretning af abonnenter eller fysiske personer om brud på persondatasikkerheden

Efter forordningens artikel 3 skal udbydere af offentlige elektroniske kommunikationstjenester – ud over underretningen til Erhvervsstyrelsen – underrette abonnenter eller fysiske personer, **hvis bruddet på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred** for de pågældende. Forordningens artikel 3, stk. 2, indeholder nærmere bestemmelser om, hvad der skal tages i betragtning ved vurderingen af, om dette er tilfældet[19].

Som eksempel på en situation, hvor udbyderen skal underrette abonnenter eller fysiske personer, kan nævnes, at udbyderens it-systemer eller en medarbejder

[18] *"Væsentlige følger for driften af net og tjenester"* er defineret i § 8 i bekendtgørelse nr. 566 af 1. juni 2016.

[19] Art. 3, stk. 2, nævner bl.a. karakteren og indholdet af de pågældende persondata (fx finansielle oplysninger, særlige personfølsomme oplysninger, lokaliseringsdata, internetlogfiler, browserhistorik, e-maildata og udspecificerede opkaldslister), de sandsynlige følger af bruddet (fx om bruddet kan medføre identitetstyveri, fysisk skade eller psykologisk forstyrrelse og omstændighederne ved bruddet på persondatasikkerheden (fx hvis udbyderen er bekendt med, at de omhandlede data er i en uautoriseret tredjemands besiddelse).

hos udbyderen udleverer persondata om en abonnent til uvedkommende personer uden at sikre sig, at den pågældende er berettiget til at modtage oplysningen. Det kan fx dreje sig om udlevering af abonnenters forbrugsopgørelser eller fremsendelse af nyt password til udbyderens selvbetjeningsløsning til en anden e-mailadresse end den e-mailadresse, der er angivet i udbyderens kundesystem.

Forordningen fastsætter ikke – som ved underretning til myndigheden – et eksakt krav til, hvornår underretning til abonnenter eller fysiske personer skal ske rent tidsmæssigt. Underretningen skal ske **uden unødig forsinkelse**, efter at bruddet er påvist, og må ikke afhænge af underretningen til myndigheden. I særlige tilfælde kan underretningen af abonnenten eller den fysiske person udskydes, hvis underretning kan bringe en nødvendig undersøgelse af bruddet på persondatasikkerheden i fare. Det kan være en strafferetlig efterforskning, men også situationer, hvor det kan være hensigtsmæssigt at udskyde underretningen fx for at kunne fjerne evt. persondata fra internettet. Hvis man som udbyder er i tvivl om, hvornår underretning skal ske, kan man kontakte Erhvervsstyrelsen herom. Det er under alle omstændigheder op til den kompetente nationale myndighed (Erhvervsstyrelsen) – ud fra det enkelte tilfælde og på baggrund af omstændighederne – at tage stilling til, om myndigheden accepterer, at underretningen udskydes eller i det hele taget skal foretages[20].

Forordningens bilag II fastlægger, **hvilke oplysninger** der skal være indeholdt i en underretning af en abonnent eller en fysisk person, og det fremgår af artikel 3, stk. 4, at underretningen skal være udtrykt i et klart og letforståeligt sprog. Udbyderne må endvidere ikke bruge underretningen til at fremme eller reklamere for nye eller supplerende tjenester.

Udbyderen skal underrette abonnenten eller den fysiske person om bruddet på persondatasikkerheden med kommunikationsmidler, som sikrer en hurtig modtagelse af oplysningerne, og som er sikret i overensstemmelse med aktuelle teknikker, jf. forordningens artikel 3, stk. 6. Oplysningerne om bruddet skal stå alene og må ikke gives sammen med oplysninger om andre emner. Det fremgår således af betragtning 15 til forordningen, at fx en faktura heller ikke betragtes som et velegnet middel til at underrette om et sikkerhedsbrud.

Udgangspunktet er, at abonnenter og fysiske personer skal underrettes direkte og individuelt. Særligt i forhold til underretning af evt. berørte fysiske personer, der ikke er en given udbyders abonnenter, og som udbyderen derfor ikke har et aftaleforhold med og dermed heller ikke kontaktoplysninger om, fremgår det dog af artikel 3, stk. 7, at udbyderen kan underrette disse personer gennem annoncer i større nationale eller regionale (trykte eller elektroniske) medier i de relevante medlemsstater inden for tidsfristen. I dette tilfælde skal udbyderen videreføre rimelige bestræbelser på at identificere de pågældende fysiske personer og i givet fald hurtigst muligt underrette dem direkte efterfølgende.

Artikel 4 i forordningen indeholder en undtagelse til kravet om underretning af abonnenter eller fysiske personer. En udbyder skal således ikke underrette berørte abonnenter eller fysiske personer om et brud på persondatasikkerheden, hvis den kompetente nationale myndighed finder det godtgjort fra udbyderens side, at denne har gennemført passende teknologiske beskyttelsesforanstaltninger (fx i form af kryptering el.lign.), og at disse foranstaltninger er blevet an-

[20] Jf. forordningens betragtning 13.

vendt på de data, som sikkerhedsbruddet vedrørte. Sådanne teknologiske beskyttelsesforanstaltninger skal gøre dataene uforståelige for alle, der ikke har lovlig adgang hertil. Artikel 4, stk. 2, præciserer, hvornår data anses for uforståelige[21].

Hvis en udbyder indgår en kontrakt med en anden udbyder om at levere en del af de elektroniske kommunikationstjenester uden at have et direkte kontraktforhold til abonnenter, skal denne anden udbyder øjeblikkeligt oplyse den kontraherende udbyder om brud på persondatasikkerheden, jf. forordningens artikel 5. Bestemmelsen er uddybet i forordningens betragtning 18. Det følger heraf, at hvis en udbyder – fx en såkaldt service provider - benytter en anden udbyder til at udføre en del af tjenesteydelsen, fx i forbindelse med fakturering og ledelsesfunktioner, bør denne anden udbyder, som ikke har et direkte kontraktforhold til slutbrugeren, ikke være forpligtet til at foretage underretninger i tilfælde af brud på persondatasikkerheden. Den anden udbyder bør i stedet advare og oplyse den udbyder, der har det direkte aftaleforhold med abonnenterne, således at denne kan foretage underretningen. Dette bør i henhold til den nævnte betragtning i forordningen også gælde i forbindelse med engrosudbud af elektroniske kommunikationstjenester, hvor engrosudbyderen normalt ikke har et direkte kontraktforhold til slutbrugeren.

5.2.4. Krav om underretning til abonnenter eller fysiske personer, hvis denne ikke er sket

Hvis Erhvervsstyrelsen konstaterer, at en udbyder ikke har underrettet evt. berørte abonnenter eller fysiske personer, kan Erhvervsstyrelsen – efter at have vurderet de sandsynlige negative virkninger af bruddet – kræve, at udbyderen underretter abonnenten eller den fysiske person om sikkerhedsbruddet, jf. bekendtgørelsens § 5, stk. 2.

6. Optegnelser over brud på persondatasikkerheden – Bekendtgørelsens § 6

Det følger af bekendtgørelsens § 6, at udbydere af offentlige elektroniske kommunikationstjenester skal føre optegnelser over brud på persondatasikkerheden. Disse optegnelser skal indeholde oplysninger om omstændighederne ved bruddene, deres virkninger og de afhjælpende foranstaltninger, der er truffet. Optegnelserne skal være så detaljerede, at Erhvervsstyrelsen som led i sit tilsyn kan føre kontrol med overholdelsen af forordningens underretningskrav.

Der er ikke specifikke krav til, hvor længe optegnelserne skal gemmes og kunne fremvises. Det fremgår af betragtning 58 til den ændring af e-databeskyttel-sesdirektivet, der blev gennemført i 2009, at formålet med kravet om at føre optegnelser over brud er at give de kompetente nationale myndigheder

[21] Det fremgår af art. 4, stk. 2, at data anses for uforståelige, hvis de er blevet krypteret på sikker vis med en standardiseret algoritme, dekrypteringsnøglen ikke er kompromitteret af et brud på sikkerheden, og dekrypteringsnøglen er genereret på en sådan måde, at den ikke kan afsløres med de tilgængelige tekniske midler af en person, der ikke har lovlig adgang til nøglen, eller b) de er blevet erstattet af deres hashværdi, der beregnes med en standardiseret kryptografisk hashfunktion med en nøgle, den nøgle, der er anvendt til at hashe dataene, ikke er kompromitteret af et brud på sikkerheden, og den nøgle, der er anvendt til at hashe dataene, er genereret på en sådan måde, at den ikke kan afsløres med de tilgængelige tekniske midler af en person, der ikke har lovlig adgang til nøglen.

mulighed for at foretage yderligere analyser og evalueringer over trufne foranstaltninger og for at kunne videreformidle bedste praksis blandt udbydere. Erhvervsstyrelsen vil selv ligge inde med oplysninger vedrørende de brud, udbyderne har indberettet.

7. Tilsyn – Bekendtgørelsens §§ 7-9

Erhvervsstyrelsen fører tilsyn med, at udbydere af offentlige elektroniske kommunikationstjenester overholder de forpligtelser, de er pålagt efter bekendtgørelsen. Styrelsen kan i den forbindelse påbyde en udbyder at gennemføre tiltag, som styrelsen vurderer, er nødvendige for at sikre, at kravene om passende tekniske og organisatoriske foranstaltninger er overholdt. Erhvervsstyrelsen vil i den forbindelse skulle iagttage almindelige principper om proportionalitet og vil kun kunne påbyde at gennemføre foranstaltninger, der er nødvendige for at leve op til formålet med bekendtgørelsens krav.

Styrelsen fører også tilsyn med, at udbydere af offentlige elektroniske kommunikationstjenester overholder kravene om underretning om brud på persondatasikkerheden, som følger af Kommissionens forordning herom.

Klager over Erhvervsstyrelsens afgørelser kan indbringes for Teleklagenævnet.

8. Straf – Bekendtgørelsens § 10

Overtrædelse af bekendtgørelsens regler om risikostyring, information til brugere ved særlig risiko for brug på persondatasikkerheden, optegnelser over brud på persondatasikkerheden eller manglede efterlevelse af påbud efter bekendtgørelsen kan straffes med bøde.

Selskaber mv. kan pålægges strafansvar i medfør af reglerne i straffelovens kap. 5 vedrørende strafansvar for juridiske personer.