ARTIKEL 29-GRUPPEN VEDRØRENDE DATABESKYTTELSE

18/DA

WP250rev.01

Retningslinjer om anmeldelse af brud på persondatasikkerheden i henhold til forordning 2016/679

Vedtaget den 3. oktober 2017

Som senest revideret og vedtaget den 6. februar 2018

GRUPPEN VEDRØRENDE BESKYTTELSE AF PERSONER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER,

som er nedsat ved Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995,

som henviser til artikel 29 og 30 i ovennævnte direktiv, og

som henviser til gruppens forretningsorden,

HAR VEDTAGET FØLGENDE RETNINGSLINJER:

INDHOLDSFORTEGNELSE TOC

INDLEDNING

Den generelle forordning om databeskyttelse (GDPR) indfører kravet om, at brud på persondatasikkerheden (herefter "brud") skal anmeldes til den kompetente nationale tilsynsmyndighed[1] (eller ved brud på tværs af landegrænserne til den ledende tilsynsmyndighed), og at de personer, hvis personoplysninger er berørt af bruddet, i visse tilfælde skal underrettes om bruddet.

Forpligtelsen til anmeldelse af brud gælder for øjeblikket for visse organisationer, såsom udbydere af offentligt tilgængelige elektroniske kommunikationstjenester (som nævnt i direktiv 2009/136/EF og forordning (EU) nr. 611/2013)[2]. Der er også nogle EU-medlemsstater, der allerede har indført deres egen nationale forpligtelse til anmeldelse af brud. Dette kan omfatte en forpligtelse til at anmelde brud, som ud over udbydere af offentligt tilgængelige elektroniske kommunikationstjenester involverer kategorier af dataansvarlige (f.eks. i Tyskland og Italien), eller en forpligtelse til at rapportere alle brud, der involverer personoplysninger (som i Nederlandene). Andre medlemsstater har indført relevante adfærdskodekser (f.eks. i Irland[3]). En række EU-databeskyttelsesmyndigheder opfordrer for øjeblikket de dataansvarlige til at rapportere brud, men direktiv 95/46/EF[4] om databeskyttelse, som GDPR erstatter, indeholder ikke nogen specifik forpligtelse til anmeldelse af brud, og derfor vil dette krav være nyt for mange organisationer. GDPR gør nu anmeldelse obligatorisk for alle dataansvarlige, medmindre bruddet sandsynligvis ikke indebærer en risiko for personers rettigheder eller frihedsrettigheder[5]. Databehandlerne spiller også en væsentlig rolle, og de skal underrette deres dataansvarlige om alle brud[6].

Artikel 29-Gruppen mener, at det nye krav om anmeldelse indebærer en række fordele. Når de dataansvarlige anmelder brud til tilsynsmyndigheden, kan de få oplysninger om, hvorvidt de berørte personer skal underrettes. Tilsynsmyndigheden kan kræve, at den dataansvarlige underretter de berørte personer om bruddet[7]. Når den dataansvarlige underretter de berørte personer om et brud, kan han eller hun samtidig oplyse dem om de med bruddet forbundne risici og de forholdsregler, personerne kan træffe for at beskytte sig selv mod bruddets potentielle konsekvenser. Enhver beredskabsplan i forbindelse med brud bør fokusere på at beskytte de berørte personer og deres personoplysninger. Anmeldelse af brud bør således opfattes som et værktøj, der forbedrer regeloverholdelsen med hensyn til beskyttelse af personoplysninger. På samme tid skal det bemærkes, at manglende rapportering af brud til en person eller tilsynsmyndighed kan betyde, at den dataansvarlige kan sanktioneres, jf. artikel 83.

---

[1] Se artikel 4, stk. 21, i GDPR.

[2] Se http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex:32009L0136 og http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX%3A32013R0611.

[3] Se https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm.

[4] Se http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=celex:31995L0046.

[5] Rettigheder nedfældet i Den Europæiske Unions charter om grundlæggende rettigheder, som findes på http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=CELEX:12012P/TXT.

[6] Se artikel 33, stk. 2. Denne idé stemmer overens med idéen i artikel 5 i forordning (EU) nr. 611/2013, hvor det hedder, at en udbyder, der har indgået en kontrakt om at levere en del af en elektronisk kommunikationstjeneste (uden at have et direkte kontraktforhold til abonnenter), skal oplyse den kontraherende udbyder om brud på persondatasikkerheden.

[7] Se artikel 34, stk. 4, og artikel 58, stk. 2, litra e).

Dataansvarlige og databehandlere opfordres derfor til på forhånd at planlægge og indføre processer, så de kan afsløre og omgående inddæmme et brud, vurdere risikoen for personer[8] og efterfølgende fastslå, om det er nødvendigt at anmelde bruddet til den kompetente tilsynsmyndighed, samt underrette de berørte personer om bruddet, når dette er nødvendigt. Anmeldelsen til tilsynsmyndigheden skal indgå i denne beredskabsplan.

GDPR indeholder bestemmelser om, hvornår et brud skal anmeldes og til hvem, samt om, hvilke oplysninger der skal gives i forbindelse med anmeldelsen. Oplysningerne kan gives trinvist, men de dataansvarlige skal under alle omstændigheder reagere rettidigt på et brud.

I sin udtalelse 03/2014 om underretning om brud på persondatasikkerheden[9] udstak Artikel 29-Gruppen retningslinjer for dataansvarlige for at hjælpe dem med at afgøre, om registrerede skal underrettes i tilfælde af brud. Udtalelsen omhandlede forpligtelserne for udbydere af elektroniske kommunikationstjenester i medfør af direktiv 2002/58/EF og indeholdt eksempler fra forskellige sektorer, som var relevante for det, der dengang var et udkast til GDPR, og beskrev god praksis for alle dataansvarlige.

De nuværende retningslinjer giver en forklaring af de obligatoriske anmeldelses- og underretningskrav vedrørende brud i GDPR samt nogle af de tiltag, dataansvarlige og -behandlere kan iværksætte for at opfylde disse nye forpligtelser. De indeholder endvidere eksempler på forskellige typer brud og på, hvem der skal underrettes i de forskellige scenarier.

I. Brud på persondatasikkerheden i henhold til GDPR

A. Grundlæggende sikkerhedshensyn

Et af kravene i GDPR er, at personoplysninger skal behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger[10].

Det betyder, at både de dataansvarlige og databehandlerne i henhold til GDPR skal have iværksat passende tekniske og organisatoriske foranstaltninger for at garantere et sikkerhedsniveau, der er passende alt efter den risiko, som behandling af personoplysninger udgør. De skal tage hensyn til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder[11]. GDPR kræver endvidere, at alle passende teknologiske beskyttelsesforanstaltninger og organisatoriske foranstaltninger er blevet gennemført, for omgående at

[8] Dette kan sikres ved overholdelse af kravet om tilsyn og revision i forbindelse med en konsekvensanalyse vedrørende databeskyttelse, som er påkrævet, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder (artikel 35, stk. 1 og 11).

[9] Se udtalelse 03/2014 om underretning om brud på persondatasikkerheden (http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_da.pdf).

[10] Se artikel 5, stk. 1, litra f), og artikel 32.

[11] Artikel 32. Se også betragtning 83.

kunne fastslå, om et brud på persondatasikkerheden har fundet sted, hvilket efterfølgende bestemmer, om anmeldelsesforpligtelsen finder anvendelse[12].

Det betyder, at et centralt element i enhver datasikkerhedspolitik er i videst muligt omfang at være i stand til at forhindre et brud, og når et sådant brud alligevel opstår, at reagere rettidigt på det.

B. Hvad er et brud på persondatasikkerheden?

1. Definition

For at kunne håndtere et brud skal den dataansvarlige først være i stand til at genkende et brud. I GDPR defineres "brud på persondatasikkerheden" i artikel 4, stk. 12, som:

> "et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet".

Meningen med "tilintetgørelse" burde være ret klar. Det er, når oplysningerne ikke længere findes eller ikke længere findes i en form, som den dataansvarlige kan bruge. Betydningen af "beskadigelse" burde også være relativt klar. Det er, når personoplysningerne er blevet ændret, ødelagt eller ikke længere er fuldstændige. "Tab" af personoplysninger skal fortolkes således, at oplysningerne måske stadig findes, men at den dataansvarlige har mistet kontrollen over eller adgangen til dem eller ikke længere er i besiddelse af dem. Endelig kan uautoriseret eller ulovlig behandling omfatte videregivelse af (eller adgang til) personoplysninger til/for modtagere, som ikke er autoriseret til at modtage (eller få adgang til) oplysningerne, og alle andre former for behandling i modstrid med GDPR.

Eksempel

Et eksempel på tab af personoplysninger er, når udstyr, som indeholder en kopi af en dataansvarligs kundedatabase, er blevet tabt eller stjålet. Et andet eksempel på tab er, når den eneste kopi af et sæt personoplysninger er blevet krypteret af ransomware eller er blevet krypteret af den dataansvarlige med en kode, som denne ikke længere er i besiddelse af.

Det, der er vigtigt, er, at et brud er en slags sikkerhedshændelse. Som det fremgår af artikel 4, stk. 12, finder GDPR dog kun anvendelse, når der er tale om brud på *personoplysninger*. Konsekvensen af et sådant brud er, at den dataansvarlige ikke er i stand til at sikre overholdelsen af principperne for behandling af personoplysninger, jf. artikel 5 i GDPR. Dette understreger forskellen på en sikkerhedshændelse og et brud på persondatasikkerheden. Grundlæggende er alle brud på persondatasikkerheden sikkerhedshændelser, mens sikkerhedshændelser ikke nødvendigvis er brud på persondatasikkerheden[13].

Et bruds potentielle skadevirkninger for personer behandles nedenfor.

2. Forskellige typer brud på persondatasikkerheden

[12] Se betragtning 87.

[13] Det skal bemærkes, at sikkerhedshændelser ikke er begrænset til trusselsmodeller, hvor en ekstern kilde retter et angreb mod en organisation, men også omfatter hændelser, hvor intern behandling er i modstrid med sikkerhedsprincipperne.

I sin udtalelse 03/2014 om underretning om brud forklarede Artikel 29-Gruppen, at brud kan kategoriseres efter følgende tre velkendte informationssikkerhedsprincipper[14]:

- "Brud på fortrolighed" – når der foreligger uautoriseret eller hændelig videregivelse af eller adgang til personoplysninger.
- "Brud på integritet" – når der foreligger uautoriseret eller hændelig ændring af personoplysninger.
- "Brud på tilgængelighed" – når der foreligger hændeligt eller uautoriseret tab af adgang[15] til eller tilintetgørelse af personoplysninger.

Det skal endvidere bemærkes, at et brud alt efter omstændighederne kan vedrøre personoplysningers fortrolighed, integritet og tilgængelighed på samme tid eller en kombination af disse.

Mens det er forholdsvis enkelt at fastslå, om der foreligger et brud på fortroligheden eller integriteten, kan det være mere kompliceret at fastslå, om der foreligger et brud på tilgængeligheden. Et brud vil altid blive opfattet som et brud på tilgængeligheden, når personoplysninger er blevet tabt permanent eller er blevet tilintetgjort.

Eksempel

Eksemplerne på tab af tilgængelighed omfatter tilfælde, hvor oplysninger er blevet slettet enten utilsigtet eller af en uautoriseret person, eller hvor oplysninger er blevet sikkert krypteret, men man har mistet dekrypteringskoden. Såfremt den dataansvarlige ikke kan genoprette adgangen til oplysningerne fra f.eks. en backup, opfattes det som et permanent tab af tilgængelighed.

Et tab af tilgængelighed kan også foreligge, når der har været en omfattende forstyrrelse af en organisations almindelige tjeneste, f.eks. ved en strømafbrydelse eller et Denial of Service-angreb, som gør personoplysningerne utilgængelige.

Spørgsmålet er, om et midlertidigt tab af tilgængelighed for personoplysninger skal opfattes som et brud, og om det i så fald er et brud, der skal anmeldes. I artikel 32 i GDPR om behandlingssikkerhed forklares det, at der ved gennemførelse af tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til risiciene, bl.a. skal tages hensyn til "evne[n] til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester" og "evne[n] til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse".

Derfor er en sikkerhedshændelse, der resulterer i, at personoplysninger ikke er tilgængelige i et vist tidsrum, også en slags brud, da den manglende adgang til oplysningerne kan have stor indvirkning på fysiske personers rettigheder og frihedsrettigheder. For at gøre det helt klart udgør tilfælde, hvor personoplysninger ikke er tilgængelige som følge af udførelsen af planlagt systemvedligeholdelse, ikke et "brud på sikkerheden", jf. artikel 4, stk. 12.

[14] Se udtalelse 03/2014.

[15] Det ligger fast, at "adgang" grundlæggende er en del af "tilgængelighed". Se f.eks. NIST SP800-53rev4, hvor "tilgængelighed" (availability) defineres som sikring af rettidig og pålidelig adgang til og anvendelse af oplysninger (Ensuring timely and reliable access to and use of information), findes på http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. I CNSSI-4009 henvises der også til "Rettidig, pålidelig adgang til data og informationstjenester for godkendte brugere." Se https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 definerer også "tilgængelighed" som det forhold at være tilgængeligt og anvendeligt efter anmodning fra en autoriseret enhed (Property of being accessible and usable upon demand by an authorized entity): https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

Som med et permanent tab eller tilintetgørelse af personoplysninger (eller en hvilken som helst anden form for brud) skal et brud, der medfører midlertidigt tab af tilgængelighed, dokumenteres i henhold til artikel 33, stk. 5. Dette hjælper den dataansvarlige med at bevise sin ansvarlighed over for tilsynsmyndigheden, som kan bede om at se fortegnelser herover[16]. Alt efter omstændighederne omkring et brud kan det være nødvendigt at anmelde bruddet til tilsynsmyndigheden og underrette de berørte personer herom. Den dataansvarlige skal vurdere sandsynligheden for og alvoren af indvirkningen på fysiske personers rettigheder og frihedsrettigheder som følge af personoplysningernes manglende tilgængelighed. I henhold til artikel 33 skal den dataansvarlige anmelde bruddet, medmindre det er usandsynligt, at bruddet indebærer en risiko for personers rettigheder og frihedsrettigheder. Dette skal naturligvis vurderes i hver enkelt sag.

Eksempler

På et hospital kan det indebære en risiko for personers rettigheder og frihedsrettigheder, hvis kritiske helbredsoplysninger om patienter ikke er tilgængelige, selv midlertidigt. Det kan f.eks. betyde, at operationer bliver aflyst, og at menneskeliv bringes i fare.

Omvendt er det usandsynligt, at det forhold, at en medievirksomheds systemer ikke er tilgængelige i nogle timer (f.eks. på grund af en strømafbrydelse), og at virksomheden derfor ikke kan sende nyhedsbreve ud til sine abonnenter, indebærer en risiko for personers rettigheder og frihedsrettigheder.

Det skal bemærkes, at selv om den manglende tilgængelighed af en dataansvarligs systemer kun er midlertidig og ikke har nogen virkning for personer, er det vigtigt, at den dataansvarlige tager højde for alle potentielle konsekvenser af et brud, da det stadig kan være nødvendigt at anmelde bruddet af andre årsager.

Eksempel

Ransomware-inficering (skadelig software, som krypterer den dataansvarliges data, indtil der betales en løsesum ("ransom")) kan medføre midlertidigt tab af tilgængelighed, hvis dataene kan gendannes fra backuppen. Der har imidlertid fundet en netværksindtrængen sted, og anmeldelse kan være påkrævet, hvis hændelsen kvalificeres som et brud på fortroligheden (dvs. at angriberen har fået adgang til personoplysninger), og dette indebærer en risiko for personers rettigheder og frihedsrettigheder.

3. Potentielle konsekvenser af et brud på persondatasikkerheden

Et brud kan potentielt have en række omfattende skadevirkninger for personer, som kan føre til fysisk, materiel eller immateriel skade. GDPR forklarer, at dette kan omfatte tab af kontrol over deres personoplysninger, begrænsning af deres rettigheder, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, uautoriseret ophævelse af pseudonymisering, skade på omdømme og tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt. Det kan også indebære betydelige økonomiske eller sociale konsekvenser for de berørte personer[17].

GDPR kræver derfor, at den dataansvarlige anmelder et brud til den kompetente tilsynsmyndighed, medmindre det er usandsynligt, at det indebærer en risiko for, at sådanne skadevirkninger vil opstå.

[16] Se artikel 33, stk. 5.

[17] Se også betragtning 85 og 75.

Når der sandsynligvis er en høj risiko for, at disse skadevirkninger vil opstå, kræver GDPR, at den dataansvarlige underretter de berørte personer om bruddet, så snart det med rimelighed er muligt[18].

Vigtigheden af at kunne identificere et brud, vurdere risikoen for personer og om nødvendigt anmelde bruddet understreges i betragtning 87 i GDPR:

> "Det bør undersøges, om alle passende teknologiske beskyttelsesforanstaltninger og organisatoriske foranstaltninger er blevet gennemført, for omgående at kunne fastslå, om et brud på persondatasikkerheden har fundet sted, og for straks at kunne informere tilsynsmyndigheden og den registrerede. Om anmeldelsen fandt sted uden unødig forsinkelse bør fastslås, under særlig hensyntagen til karakteren og alvoren af bruddet på persondatasikkerheden og dets konsekvenser og skadevirkninger for den registrerede. En sådan anmeldelse kan føre til indgriben fra tilsynsmyndigheden i overensstemmelse med dens opgaver og beføjelser i henhold til denne forordning."

Der findes yderligere retningslinjer om vurdering af risikoen for skadevirkninger for personer i afsnit IV.

Hvis de dataansvarlige undlader at anmelde brud på datasikkerheden til enten tilsynsmyndigheden eller de registrerede eller begge, selv om kravene i artikel 33 og/eller 34 er opfyldt, træffer tilsynsmyndigheden et valg, hvor den tager hensyn til alle de korrigerende foranstaltninger, den har til rådighed, herunder pålæggelse af en passende administrativ bøde[19], enten i tillæg til en korrigerende foranstaltning i artikel 58, stk. 2, eller alene. Når det vælges at pålægge den dataansvarlige en administrativ bøde, kan den være på op til 10 000 000 EUR eller op til 2 % af en virksomheds samlede globale årlige omsætning, jf. artikel 83, stk. 4, litra a), i GDPR. Det er også vigtigt at huske på, at manglende anmeldelse af et brud i nogle tilfælde kan være tegn på enten manglende eller utilstrækkelige eksisterende sikkerhedsforanstaltninger. I Artikel 29-Gruppens retningslinjer om administrative bøder hedder det, at hvis flere forskellige overtrædelser, der er begået samtidig, forekommer i en bestemt sag, betyder det, at tilsynsmyndigheden kan fastsætte administrative bøder på et niveau, som er effektivt, står i rimeligt forhold til overtrædelsens alvor og har afskrækkende virkning, inden for grænserne af den alvorligste overtrædelse. I dette tilfælde har tilsynsmyndigheden også mulighed for at pålægge sanktioner for manglende anmeldelse af eller underretning om bruddet (artikel 33 og 34) på den ene side og manglende (tilstrækkelige) sikkerhedsforanstaltninger (artikel 32) på den anden side, da der er tale om to separate overtrædelser.

II. Artikel 33 – Anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden

A. Hvornår skal brud anmeldes?

1. Krav i artikel 33

Artikel 33, stk. 1, bestemmer, at:

[18] Se også betragtning 86.

[19] Der findes yderligere oplysninger i Artikel 29-Gruppens retningslinjer om anvendelse og fastsættelse af administrative bøder (WP29 Guidelines on the application and setting of administrative fines) på: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

"Ved brud på persondatasikkerheden anmelder den dataansvarlige uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det, bruddet på persondatasikkerheden til den tilsynsmyndighed, som er kompetent i overensstemmelse med artikel 55, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen."

Betragtning 87 lyder som følger[20]:

"Det bør undersøges, om alle passende teknologiske beskyttelsesforanstaltninger og organisatoriske foranstaltninger er blevet gennemført, for omgående at kunne fastslå, om et brud på persondatasikkerheden har fundet sted, og for straks at kunne informere tilsynsmyndigheden og den registrerede. Om anmeldelsen fandt sted uden unødig forsinkelse bør fastslås, under særlig hensyntagen til karakteren og alvoren af bruddet på persondatasikkerheden og dets konsekvenser og skadevirkninger for den registrerede. En sådan anmeldelse kan føre til indgriben fra tilsynsmyndigheden i overensstemmelse med dens opgaver og beføjelser i henhold til denne forordning."

2. Hvornår bliver en dataansvarlig "bekendt" med et brud?

Som anført ovenfor kræves det i GDPR, at den dataansvarlige ved brud på persondatasikkerheden anmelder brud uden unødig forsinkelse og om muligt senest 72 timer, efter at denne er blevet bekendt med det. Dette kan rejse spørgsmålet om, hvornår en dataansvarlig kan menes at være blevet "bekendt" med et brud. Artikel 29-Gruppen mener, at en dataansvarlig bør opfattes som værende "bekendt" med et brud, når denne har en rimelig grad af vished om, at der er opstået en sikkerhedshændelse, som kompromitterer personoplysninger.

Som nævnt tidligere kræves det i GDPR, at den dataansvarlige gennemfører alle passende teknologiske beskyttelsesforanstaltninger og organisatoriske foranstaltninger for omgående at kunne fastslå, om et brud har fundet sted, og for straks at kunne informere tilsynsmyndigheden og de registrerede. I forordningen hedder det endvidere, at det bør fastslås, om anmeldelsen fandt sted uden unødig forsinkelse, under særlig hensyntagen til karakteren og alvoren af bruddet på persondatasikkerheden og dets konsekvenser og skadevirkninger for den registrerede[21]. Dette forpligter den dataansvarlige til at sørge for, at denne bliver "bekendt" med brud rettidigt og dermed kan træffe passende foranstaltninger.

Nøjagtig hvornår en dataansvarlig kan opfattes som værende "bekendt" med et bestemt brud på persondatasikkerheden afhænger af omstændighederne omkring det specifikke brud. I nogle tilfælde er det allerede fra starten relativt klart, at der er opstået et brud, mens det i andre tilfælde kan tage tid at fastslå, om personoplysninger er blevet kompromitteret. Det vigtigste er dog, at en hændelse undersøges hurtigt for at fastslå, hvorvidt der er sket et brud på persondatasikkerheden, og i påkommende tilfælde iværksætte afhjælpende foranstaltninger og eventuelt anmeldelse.

Eksempler

1. I et tilfælde, hvor en USB-nøgle med ikkekrypterede personoplysninger bliver tabt, er det ofte ikke muligt at vurdere, om uautoriserede personer har fået adgang til oplysningerne. Selv om den

[20] Betragtning 85 er også vigtig her.

[21] Se betragtning 87.

dataansvarlige måske ikke er i stand til at fastslå, om der er sket et brud på fortroligheden, skal et sådant tilfælde ikke desto mindre anmeldes, da der er en rimelig grad af vished for, at der er opstået et brud på tilgængeligheden. Den dataansvarlige bliver "bekendt" med bruddet, når denne opdager, at USB-nøglen er blevet tabt.

2. En tredjemand underretter en dataansvarlig om, at han eller hun utilsigtet har modtaget personoplysninger om en af den dataansvarliges kunder, og forelægger bevis for den uautoriserede videregivelse. Da den dataansvarlige har fået forelagt et klart bevis for et brud på fortroligheden, kan der ikke herske nogen tvivl om, at denne er blevet "bekendt" med bruddet.

3. En dataansvarlig opdager, at en person kan være trængt ind i virksomhedens netværk. Den dataansvarlige gennemgår sine systemer for at fastslå, om personoplysninger i det pågældende system er blevet kompromitteret, og bekræfter, at dette er tilfældet. Igen kan der her ikke herske nogen tvivl om, at den dataansvarlige er blevet "bekendt" med bruddet, da der findes et klart bevis herfor.

4. En IT-kriminel kontakter den dataansvarlige efter at have hacket dennes system for at kræve en løsesum. I dette tilfælde har den dataansvarlige – efter at have undersøgt sit system for at få bekræftet, at det er blevet angrebet – et klart bevis for, at der er sket et brud, og der er derfor ingen tvivl om, at den dataansvarlige er blevet "bekendt" med det.

Når en dataansvarlig først er blevet underrettet om et potentielt brud af en person, en medieorganisation eller en anden kilde, eller når den dataansvarlige selv har opdaget en sikkerhedshændelse, har denne et kort tidsrum til at undersøge sagen for at fastslå, om der rent faktisk er sket et brud. I dette tidsrum kan den dataansvarlige ikke anses for at være "bekendt" med bruddet. Det forventes imidlertid, at den indledende undersøgelse finder sted hurtigst muligt og med en rimelig grad af sikkerhed fastslår, om et brud har fundet sted. Derefter kan der foretages en mere tilbundsgående undersøgelse.

Når den dataansvarlige er blevet bekendt med bruddet, skal bruddet, når dette er påkrævet, anmeldes uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med det. I dette tidsrum bør den dataansvarlige vurdere den sandsynlige risiko for personer med henblik på at fastslå, om anmeldelseskravet er udløst, og hvilke foranstaltninger der skal træffes for at håndtere bruddet. En dataansvarlig kan dog allerede få foretaget en foreløbig vurdering af den potentielle risiko, som et brud kan indebære, som led i en konsekvensanalyse vedrørende databeskyttelse[22], inden den dataansvarlige indleder den pågældende behandlingsoperation. Konsekvensanalysen vedrørende databeskyttelse kan dog være mere generel sammenholdt med de specifikke forhold omkring et brud, så der skal under alle omstændigheder foretages en supplerende vurdering, som tager højde for disse forhold. Der findes yderligere oplysninger om risikovurdering i afsnit IV.

I de fleste tilfælde bør disse foreløbige foranstaltninger gennemføres straks efter den første advarsel (dvs. når den dataansvarlige eller databehandleren får mistanke om en sikkerhedshændelse, som kan involvere personoplysninger) – det bør kun tage længere tid i ekstraordinære tilfælde.

Eksempel

En person underretter den dataansvarlige om, at han eller hun har modtaget en e-mail fra en person, der foregiver at være den dataansvarlige. E-mailen indeholder personoplysninger vedrørende personens (faktiske) anvendelse af den dataansvarliges tjeneste, hvilket tyder på, at den

[22] Se Artikel 29-Gruppens retningslinjer om konsekvensanalyser vedrørende databeskyttelse her: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

dataansvarliges sikkerhed er blevet kompromitteret. Den dataansvarlige undersøger hurtigt sagen og identificerer en indtrængen i netværket og bevis for uautoriseret adgang til personoplysninger. Den dataansvarlige anses nu for at være "bekendt" med bruddet og skal anmelde det til tilsynsmyndigheden, medmindre det sandsynligvis ikke indebærer en risiko for personers rettigheder og frihedsrettigheder. Den dataansvarlige skal træffe passende afhjælpende foranstaltninger for at håndtere bruddet.

Den dataansvarlige bør derfor have indført interne processer for detektering og håndtering af brud. For at finde uregelmæssigheder i databehandlingen kan den dataansvarlige eller databehandleren f.eks. anvende bestemte tekniske midler såsom dataudvekslings- og loganalyseprogrammer, ud fra hvilke det er muligt at identificere hændelser og advarsler ved at sammenholde logdata[23]. Det er vigtigt, at et brud, når det detekteres, rapporteres opad til det relevante ledelsesniveau, så det kan blive håndteret og om nødvendigt anmeldt, jf. artikel 33 og eventuelt artikel 34. Disse tekniske midler og rapporteringsmekanismer kan fastlægges i den dataansvarliges beredskabsplan og/eller forvaltningssystemer. De vil hjælpe den dataansvarlige med at planlægge effektivt og fastslå, hvem i organisationen der har det operationelle ansvar for håndtering af brud, og hvordan eller hvorvidt en hændelse skal formidles videre.

Den dataansvarlige bør også have indgået aftaler med de databehandlere, den dataansvarlige benytter sig af, som selv er forpligtede til at underrette den dataansvarlige om brud (jf. nedenfor).

Mens det er de dataansvarliges og databehandlernes ansvar at iværksætte passende foranstaltninger for at forebygge, reagere på og håndtere brud, er der en række praktiske tiltag, der bør iværksættes i alle tilfælde.

- Oplysninger om alle sikkerhedsrelaterede hændelser bør formidles videre til en ansvarlig person eller til personer, der har til opgave at håndtere hændelser, fastslå, at der foreligger et brud, og vurdere risici.
- Dernæst bør den risiko, som et brud indebærer for personer, vurderes (sandsynlighed for ingen risiko, risiko eller høj risiko), og organisationens relevante afdelinger bør underrettes.
- Bruddet anmeldes til tilsynsmyndigheden, og de berørte personer underrettes om bruddet, hvis dette er påkrævet.
- På samme tid bør den dataansvarlige inddæmme og afhjælpe bruddet.
- Bruddet bør dokumenteres i takt med, at det udvikler sig.

Det bør tilsvarende stå klart, at den dataansvarlige er forpligtet til at reagere på enhver indledende advarsel og fastslå, om der rent faktisk er opstået et brud eller ej. I dette korte tidsrum kan der foretages enkelte undersøgelser, og den dataansvarlige kan indsamle beviser og andre relevante oplysninger. Men så snart den dataansvarlige med en rimelig grad af sikkerhed har fastslået, at der er sket et brud, og betingelserne i artikel 33, stk. 1, er opfyldt, skal denne anmelde bruddet til tilsynsmyndigheden uden unødig forsinkelse og om muligt senest inden for 72 timer[24]. Hvis ikke den dataansvarlige reagerer rettidigt, og det viser sig, at der er sket et brud, kan dette opfattes som manglende anmeldelse, jf. artikel 33.

I artikel 32 slås det fast, at den dataansvarlige og databehandleren bør gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et passende sikkerhedsniveau for personoplysninger.

[23] Det skal bemærkes, at logdata, som letter kontrol af f.eks. opbevaring, ændring eller sletning af oplysninger, også kan opfattes som personoplysninger vedrørende den person, der indledte den pågældende behandlingsoperation.

[24] Se forordning nr. 1182/71 om fastsættelse af regler om tidsfrister, datoer og tidspunkter på: http://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:31971R1182&from=DA

Evnen til at detektere, håndtere og rapportere et brud rettidigt bør ses som et afgørende element af disse foranstaltninger.

3. Fælles dataansvarlige

Artikel 26 vedrører fælles dataansvarlige og fastslår, at fælles dataansvarlige fastlægger deres respektive ansvar for overholdelse af GDPR[25]. Dette indebærer fastlæggelse af, hvilken part der er ansvarlig for overholdelse af forpligtelserne i artikel 33 og 34. Artikel 29-Gruppen anbefaler, at kontrakten mellem de fælles dataansvarlige indeholder bestemmelser, som fastlægger, hvilken dataansvarlig der fører an med hensyn til eller er ansvarlig for overholdelse af forpligtelserne til anmeldelse af brud i GDPR.

4. Databehandlerens forpligtelser

Den dataansvarlige har det overordnede ansvar for beskyttelse af personoplysninger, men databehandleren spiller en væsentlig rolle for, at den dataansvarlige kan overholde sine forpligtelser, og denne rolle omfatter bl.a. underretning om brud. I artikel 28, stk. 3, fastlægges det, at en databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument. I artikel 28, stk. 3, litra f), hedder det, at kontrakten eller det andet retlige dokument fastsætter, at databehandleren "bistår den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren".

Artikel 33, stk. 2, gør det klart, at hvis den dataansvarlige gør brug af en databehandler, og databehandleren bliver bekendt med et brud vedrørende de personoplysninger, denne behandler for den dataansvarlige, skal databehandleren underrette den dataansvarlige "uden unødig forsinkelse". Det skal bemærkes, at databehandleren ikke først skal vurdere sandsynligheden for, at bruddet indebærer en risiko, inden den dataansvarlige underrettes. Det er den dataansvarlige, der skal foretage en vurdering, når denne bliver bekendt med bruddet. Databehandleren skal blot fastslå, om der er sket et brud, og så underrette den dataansvarlige. Den dataansvarlige bruger databehandleren til at nå sine mål. Derfor bør den dataansvarlige i princippet anses for at være "bekendt" med bruddet, når databehandleren har underrettet den dataansvarlige om bruddet. Databehandlerens forpligtelse til at underrette den dataansvarlige giver den dataansvarlige mulighed for at håndtere bruddet og fastslå, hvorvidt det er nødvendigt at anmelde det til tilsynsmyndigheden, jf. artikel 33, stk. 1, og underrette de berørte personer, jf. artikel 34, stk. 1. Den dataansvarlige vil muligvis gerne selv undersøge bruddet, da databehandleren ikke nødvendigvis kender til alle relevante forhold i sagen, f.eks. om den dataansvarlige stadig ligger inde med en kopi eller backup af personoplysninger, der er blevet ødelagt eller tabt hos databehandleren. Dette kan have betydning for, om den dataansvarlige skal anmelde bruddet.

GDPR fastsætter ikke nogen udtrykkelig tidsfrist for databehandlerens underretning af den dataansvarlige, kun at det skal gøres "uden unødig forsinkelse". Artikel 29-Gruppen anbefaler derfor, at databehandleren øjeblikkelig underretter den dataansvarlige og trinvis giver yderligere oplysninger om bruddet i takt med, at oplysningerne bliver tilgængelige. Dette er vigtigt for at hjælpe den dataansvarlige med at opfylde kravet om anmeldelse til tilsynsmyndigheden inden for 72 timer.

Som forklaret ovenfor bør kontrakten mellem den dataansvarlige og databehandleren fastslå, hvordan kravene i artikel 33, stk. 2, og de øvrige bestemmelser i GDPR skal overholdes. Dette kan omfatte krav om databehandlerens tidlige underretning, som således understøtter den dataansvarliges forpligtelse til at rapportere til tilsynsmyndigheden inden for 72 timer.

[25] Se også betragtning 79.

Når databehandleren leverer tjenester til flere dataansvarlige, der alle er berørt af den samme hændelse, skal databehandleren rapportere hændelsen til alle de dataansvarlige.

En databehandler kan anmelde et brud på den dataansvarliges vegne, hvis sidstnævnte har givet databehandleren behørig tilladelse hertil, og dette fremgår af kontrakten mellem den dataansvarlige og databehandleren. En sådan anmeldelse skal ske i henhold til artikel 33 og 34. Det er dog vigtigt at bemærke, at det retlige ansvar fortsat påhviler den dataansvarlige.

B. Afgivelse af oplysninger til tilsynsmyndigheden

1. Oplysninger, der skal afgives

Når en dataansvarlig anmelder et brud til tilsynsmyndigheden, hedder det i artikel 33, stk. 3, at anmeldelsen mindst skal:

> "a) beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
>
> b) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
>
> c) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
>
> d) beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.".

GDPR definerer ikke kategorierne af registrerede og registreringer af personoplysninger. Artikel 29-Gruppen foreslår dog, at kategorierne af registrerede refererer til de forskellige typer personer, hvis personoplysninger er berørt af et brud. Alt efter de anvendte deskriptorer kunne det bl.a. være børn og andre sårbare grupper, handicappede, ansatte og kunder. På samme måde kan kategorier af registreringer af personoplysninger referere til de forskellige typer registreringer, den dataansvarlige behandler, såsom oplysninger om helbred, uddannelse, social omsorg, økonomi, bankkontonumre, pasnumre osv.

Det fremgår klart af betragtning 85, at et af målene med anmeldelse er at begrænse skaden på personer. Hvis kategorierne af registrerede eller registreringer af personoplysninger indebærer en risiko for særlig skade som følge af brud (f.eks. identitetstyveri, svig, økonomisk tab, trussel mod tavshedspligt), er det vigtigt, at disse kategorier indgår i anmeldelsen. På denne måde hænger de sammen med kravet om, at de sandsynlige konsekvenser af bruddet skal beskrives.

At der ikke findes nøjagtige oplysninger (f.eks. det præcise antal berørte registrerede) bør ikke være en hindring for rettidig anmeldelse af et brud. GDPR giver plads til omtrentlig angivelse af antallet af berørte personer og antallet af berørte registreringer af personoplysninger. Der bør fokuseres på at håndtere bruddets skadevirkninger snarere end på at opgive nøjagtige tal. Når det står klart, at der er sket et brud, men omfanget af det endnu ikke er kendt, er en trinvis anmeldelse (se nedenfor) således en sikker måde at opfylde anmeldelsesforpligtelserne på.

I artikel 33, stk. 3, hedder det, at den dataansvarlige "skal mindst" oplyse dette i en anmeldelse, så en dataansvarlig kan om nødvendigt vælge at afgive yderligere oplysninger. Forskellige typer brud (fortrolighed, integritet eller tilgængelighed) kan kræve, at der afgives yderligere oplysninger for at belyse forholdene i en given sag fuldt ud.

Eksempel

I sin anmeldelse til tilsynsmyndigheden kan en dataansvarlig finde det hensigtsmæssigt at oplyse navnet på sin databehandler, hvis denne er kilden til et brud, især hvis bruddet har medført en hændelse, der påvirker registreringer af personoplysninger for mange andre dataansvarlige, som bruger den samme databehandler.

Under alle omstændigheder kan tilsynsmyndigheden anmode om yderligere oplysninger som led i sin undersøgelse af et brud.

2. Trinvis anmeldelse

Alt efter arten af et brud kan det være nødvendigt, at den dataansvarlige foretager yderligere undersøgelser for at fastslå alle relevante forhold i forbindelse med hændelsen. Artikel 33, stk. 4, bestemmer således, at:

"Når og for så vidt som det ikke er muligt at give oplysningerne samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse.".

Det betyder, at GDPR anerkender, at de dataansvarlige ikke altid har alle de nødvendige oplysninger om et brud 72 timer efter, at de er blevet bekendt med det, da der ikke altid foreligger fuldstændige og tilbundsgående oplysninger om hændelsen i denne indledende periode. Forordningen giver derfor mulighed for trinvis anmeldelse. Det er mest sandsynligt, at dette er tilfældet ved mere komplekse brud, såsom nogle former for cybersikkerhedshændelser, hvor en tilbundsgående kriminalteknisk undersøgelse kan være nødvendig for at fastslå arten af bruddet og omfanget af bruddets kompromittering af personoplysninger. I mange tilfælde vil den dataansvarlige således være nødt til at foretage flere undersøgelser og følge op med yderligere oplysninger på et senere tidspunkt. Dette er tilladt, når den dataansvarlige angiver en begrundelse for forsinkelsen, jf. artikel 33, stk. 1. Artikel 29-Gruppen anbefaler, at den dataansvarlige, når denne anmelder et brud til tilsynsmyndigheden, også nævner for tilsynsmyndigheden, hvis den dataansvarlige endnu ikke har alle de nødvendige oplysninger og vil komme med flere oplysninger senere. Tilsynsmyndigheden bør oplyse, hvordan og hvornår de yderligere oplysninger skal gives. Dette forhindrer ikke den dataansvarlige i at komme med yderligere oplysninger på et hvilket som helst tidspunkt, hvis denne bliver bekendt med supplerende relevante oplysninger om bruddet, som skal meddeles tilsynsmyndigheden.

Kravet om anmeldelse har til formål at opfordre de dataansvarlige til at reagere omgående på et brud, inddæmme det og om muligt få de kompromitterede personoplysninger tilbage, og til at anmode tilsynsmyndigheden om relevante råd. Ved at anmelde et brud til tilsynsmyndigheden inden for de første 72 timer kan den dataansvarlige sikre, at beslutningerne om, hvorvidt de berørte personer skal underrettes eller ej, er rigtige.

Formålet med at anmelde brud til tilsynsmyndigheden er dog ikke kun at få råd om, hvorvidt de berørte personer skal underrettes. Det vil i nogle tilfælde være åbenlyst, at den dataansvarlige som følge af bruddets art og risikoens alvor straks skal underrette de berørte personer. Hvis der f.eks. er en umiddelbar fare for identitetstyveri, eller hvis særlige kategorier af personoplysninger[26] er blevet offentliggjort online, bør den dataansvarlige reagere uden unødig forsinkelse for at inddæmme bruddet og underrette de berørte personer derom (se afsnit III). I ekstraordinære tilfælde kan dette endda gøres, inden bruddet anmeldes til tilsynsmyndigheden. Mere overordnet kan anmeldelse til tilsynsmyndigheden ikke bruges som en begrundelse for manglende underretning af de registrerede, når dette er påkrævet.

[26] Se artikel 9.

Det skal også slås fast, at den dataansvarlige efter en indledende anmeldelse kan kontakte tilsynsmyndigheden igen, hvis en opfølgende undersøgelse skaffer bevis for, at sikkerhedshændelsen blev inddæmmet, og der ikke skete noget reelt brud. Disse oplysninger kan så føjes til de oplysninger, tilsynsmyndigheden allerede har modtaget, og hændelsen tilsvarende registreres som en hændelse, men ikke et brud. Det sanktioneres ikke at rapportere en hændelse, der i sidste ende viser sig ikke at være et brud.

Eksempel

En dataansvarlig anmelder et brud til tilsynsmyndigheden senest 72 timer efter, at den dataansvarlige har opdaget, at der mangler en USB-nøgle med en kopi af personoplysninger om nogle af den dataansvarliges kunder. USB-nøglen bliver senere fundet i den dataansvarliges lokaler, hvor den var blevet lagt et forkert sted. Den dataansvarlige kontakter tilsynsmyndigheden og anmoder om at få ændret anmeldelsen.

Det skal bemærkes, at den trinvise tilgang til anmeldelse allerede er en del af de eksisterende forpligtelser i direktiv 2002/58/EF, forordning 611/2013 og andre forpligtelser i forbindelse med selvrapporterede hændelser.

3. Forsinket anmeldelse

I artikel 33, stk. 1, slås det fast, at foretages anmeldelsen til tilsynsmyndigheden ikke inden for 72 timer, skal den ledsages af en begrundelse for forsinkelsen. Ved denne bestemmelse og den trinvise anmeldelse anerkendes det, at en dataansvarlig ikke altid kan anmelde et brud inden for denne frist, og at det er muligt at foretage en forsinket anmeldelse.

Dette scenarie kan f.eks. opstå, når en dataansvarlig inden for et kort tidsrum oplever flere brud på fortroligheden, der ligner hinanden, og som berører et stort antal registrerede på den samme måde. En dataansvarlig kan blive bekendt med et brud, og mens den pågældende foretager sin undersøgelse, og inden bruddet anmeldes, opdage flere tilsvarende brud, som har andre årsager. Alt efter omstændighederne kan det tage et stykke tid for den dataansvarlige at fastslå omfanget af bruddene, og i stedet for at anmelde hvert enkelt brud hver for sig samler den dataansvarlige dem fornuftigt i en anmeldelse af flere brud, der ligner hinanden meget, med potentielt forskellige årsager. Dette kan betyde, at anmeldelsen til tilsynsmyndigheden forsinkes med mere end de 72 timer efter, at den dataansvarlige først blev bekendt med bruddene.

Hvert enkelt brud er strengt taget en hændelse, der skal rapporteres. Men for at undgå en overdrevent stor byrde kan den dataansvarlige indsende en samlet anmeldelse af alle disse brud, under forudsætning af at de vedrører den samme type brud på den samme type personoplysninger over et relativt kort tidsrum. Hvis der sker en række brud på forskellige typer personoplysninger, der udsættes for forskellige typer brud, bør anmeldelsen foretages som normalt, og hvert enkelt brud rapporteres i henhold til artikel 33.

GDPR giver til en vis grad mulighed for forsinket anmeldelse, men dette må ikke opfattes som noget, der sker regelmæssigt. Det er værd at bemærke, at der også kan foretages samlede anmeldelser af flere brud, der ligner hinanden, inden for 72 timer.

C. Grænseoverskridende brud og brud i virksomheder uden for EU

1. Grænseoverskridende brud

Ved grænseoverskridende behandling[27] af personoplysninger kan et brud påvirke registrerede i mere end én medlemsstat. Artikel 33, stk. 1, gør det klart, at den dataansvarlige i tilfælde af et brud bør anmelde bruddet til den tilsynsmyndighed, som er kompetent i overensstemmelse med artikel 55 i GDPR[28]. Artikel 55, stk. 1, bestemmer, at:

> "Hver tilsynsmyndighed er kompetent til at udføre de opgaver og udøve de beføjelser, der tillægges den i overensstemmelse med denne forordning, på sin egen medlemsstats område.".

Artikel 56, stk. 1, lyder imidlertid som følger:

> "Uden at det berører artikel 55 er tilsynsmyndigheden for den dataansvarliges eller databehandlerens hovedvirksomhed eller eneste etablering kompetent til at fungere som ledende tilsynsmyndighed for den grænseoverskridende behandling, der foretages af denne dataansvarlige eller databehandler efter proceduren i artikel 60."

Og i artikel 56, stk. 6, bestemmes det, at:

> "Den ledende tilsynsmyndighed er den dataansvarliges eller databehandlerens eneste kontakt i forbindelse med den grænseoverskridende behandling, der foretages af denne dataansvarlige eller databehandler.".

Det betyder, at når der sker et brud i forbindelse med grænseoverskridende behandling, og bruddet skal anmeldes, skal den dataansvarlige anmelde bruddet til den ledende tilsynsmyndighed[29]. Derfor skal en dataansvarlig ved udarbejdelsen af sin beredskabsplan i forbindelse med brud vurdere, hvilken tilsynsmyndighed der er den ledende tilsynsmyndighed, som bruddet skal anmeldes til[30]. På den måde kan den dataansvarlige reagere omgående på et brud og opfylde sine forpligtelser i henhold til artikel 33. Det bør være klart, at et brud i forbindelse med grænseoverskridende behandling skal anmeldes til den ledende tilsynsmyndighed, som ikke nødvendigvis hører hjemme på det sted, hvor de berørte registrerede befinder sig, eller hvor bruddet er opstået. Ved sin anmeldelse til den ledende tilsynsmyndighed bør den dataansvarlige angive, hvorvidt bruddet involverer virksomheder i andre medlemsstater, og i hvilke medlemsstater de registrerede sandsynligvis er blevet berørt af bruddet. Hvis den dataansvarlige er i tvivl om, hvem den ledende tilsynsmyndighed er, bør den dataansvarlige som minimum anmelde bruddet til den lokale tilsynsmyndighed på det sted, hvor bruddet opstod.

2. Brud i virksomheder uden for EU

Artikel 3 vedrører det territoriale anvendelsesområde for GDPR, herunder hvornår forordningen finder anvendelse på behandling af personoplysninger, der foretages af en dataansvarlig eller databehandler, som ikke er etableret i EU. I artikel 3, stk. 2, bestemmes det navnlig, at[31]:

---

[27] Se artikel 4, stk. 23.

[28] Se også betragtning 122.

[29] Se Artikel 29-Gruppens retningslinjer for udpegelse af en dataansvarligs eller databehandlers ledende tilsynsmyndighed (Guidelines for identifying a controller or processor's lead supervisory authority) på http://ec.europa.eu/newsroom/document.cfm?doc_id=44102.

[30] Der findes en liste med kontaktoplysninger for alle europæiske nationale databeskyttelsesmyndigheder på: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] Se også betragtning 23 og 24.

"Denne forordning finder anvendelse på behandling af personoplysninger om registrerede, der er i Unionen, og som foretages af en dataansvarlig eller databehandler, der ikke er etableret i Unionen, hvis behandlingsaktiviteterne vedrører:

a) udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet, eller

b) overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen.".

Artikel 3, stk. 3, er også relevant og lyder som følger[32]:

"Denne forordning anvendes på behandling af personoplysninger, som foretages af en dataansvarlig, der ikke er etableret i Unionen, men et sted, hvor medlemsstaternes nationale ret gælder i medfør af folkeretten."

Når en dataansvarlig, som ikke er etableret i EU, er underlagt artikel 3, stk. 2, eller artikel 3, stk. 3, og oplever et brud, er denne således stadig bundet af anmeldelsespligten i artikel 33 og 34. Artikel 27 kræver, at en dataansvarlig (og databehandler) udpeger en repræsentant i EU, hvis artikel 3, stk. 2, finder anvendelse. I sådanne tilfælde anbefaler Artikel 29-Gruppen, at brud anmeldes til tilsynsmyndigheden i den medlemsstat, hvor den dataansvarliges repræsentant i EU er etableret[33]. Når en databehandler er underlagt artikel 3, stk. 2, er denne tilsvarende bundet af de forpligtelser, der påhviler databehandlere, her navnlig forpligtelsen til at underrette den dataansvarlige om et brud, jf. artikel 33, stk. 2.

D. Forhold, hvor anmeldelse ikke er påkrævet

I artikel 33, stk. 1, gøres det klart, at når det er "usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder", er det ikke påkrævet at anmelde det til tilsynsmyndigheden. Et eksempel kunne være personoplysninger, der allerede er offentligt tilgængelige, hvor det er usandsynligt, at offentliggørelse af disse oplysninger indebærer en risiko for den berørte person. Dette står i modsætning til de eksisterende krav om anmeldelse af brud for udbydere af offentligt tilgængelige elektroniske kommunikationstjenester i direktiv 2009/136/EF, som kræver, at alle relevante brud skal anmeldes til den kompetente myndighed.

I sin udtalelse 03/2014 om underretning om brud på persondatasikkerheden[34] forklarede Artikel 29-Gruppen, at et brud på fortroligheden vedrørende personoplysninger, som var krypteret med en algoritme, der svarer til det aktuelle tekniske niveau, stadig er et brud på persondatasikkerheden og skal anmeldes. Men hvis nøglens fortrolighed er intakt, dvs. at nøglen ikke blev kompromitteret af et brud på sikkerheden og 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, er dataene i princippet uforståelige. Det er således usandsynligt, at bruddet vil være til skade for personer, og det er derfor ikke nødvendigt at underrette dem om bruddet[35]. Selv om data er krypteret, kan tab eller ændring heraf dog

[32] Se også betragtning 25.

[33] Se betragtning 80 og artikel 27.

[34] Artikel 29-Gruppens udtalelse 03/2014 om underretning om brud på persondatasikkerheden, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_da.pdf.

[35] Se også artikel 4, stk. 1 og 2, i forordning 611/2013.

have negative konsekvenser for registrerede, hvis den dataansvarlige ikke har tilstrækkelige backupper. I så fald skal de registrerede stadig underrettes, selv om dataene faktisk undergik egnede krypteringsforanstaltninger.

Artikel 29-Gruppen forklarede endvidere, at dette ligeledes ville være tilfældet hvis persondata, som f.eks. adgangskoder, var hashet og saltet på sikker vis, hvis hashværdien blev beregnet med en kryptografisk hashfunktion med en nøgle, der svarer til det aktuelle tekniske niveau, hvis den nøgle, som blev anvendt til at hashe dataene, ikke var blevet kompromitteret af et brud på sikkerheden, og hvis den nøgle, der blev anvendt til at hashe dataene, var genereret på en sådan måde, at den ikke kan afsløres med de tilgængelige tekniske midler af en person, som ikke har lovlig adgang til nøglen.

Hvis personoplysninger i betydelig grad er blevet gjort uforståelige for uautoriserede personer, og dataene er en kopi, eller der findes en backup, er det altså ikke altid nødvendigt at anmelde brud på fortroligheden af behørigt krypterede personoplysninger til tilsynsmyndigheden. Dette skyldes, at det er usandsynligt, at et sådant brud indebærer en risiko for personers rettigheder og frihedsrettigheder. Det betyder naturligvis også, at det ikke er nødvendigt at underrette de pågældende personer, da bruddet sandsynligvis ikke indebærer en høj risiko. Det bør dog erindres, at selv om det i første omgang ikke er nødvendigt at anmelde et brud, hvis det sandsynligvis ikke indebærer en risiko for personers rettigheder og frihedsrettigheder, kan dette ændre sig med tiden, hvorefter risikoen skal evalueres på ny. Hvis det efterfølgende viser sig, at nøglen er kompromitteret, eller der blotlægges en sårbarhed i krypteringssoftwaren, kan det alligevel være nødvendigt at anmelde bruddet.

Derudover skal det bemærkes, at hvis der sker et brud, og der ikke findes nogen backup af de krypterede personoplysninger, vil der være tale om et brud på tilgængeligheden, som kan indebære en risiko for personer og derfor muligvis skal anmeldes. Når der opstår et brud, som involverer tab af krypterede data, kan der, selv om der findes en backup af personoplysningerne, stadig være tale om et brud, der skal rapporteres, alt efter, hvor lang tid det tager at gendanne dataene fra backuppen, og de konsekvenser, som den manglende tilgængelighed har for de berørte personer. Som der står i artikel 32, stk. 1, litra c), er evnen "til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse" en vigtig sikkerhedsfaktor.

Eksempel

Et brud, der ikke kræver anmeldelse til tilsynsmyndigheden, kan f.eks. være tab af sikkert krypteret mobilt udstyr, der anvendes af den dataansvarlige og dennes personale. Under forudsætning af at den dataansvarlige fortsat er i besiddelse af krypteringsnøglen, og der ikke er tale om den eneste kopi af personoplysningerne, er personoplysningerne ikke tilgængelige for en angriber. Det betyder, at det er usandsynligt, at bruddet indebærer en risiko for de berørte registreredes rettigheder og frihedsrettigheder. Hvis det senere viser sig, at krypteringsnøglen er kompromitteret, eller at krypteringssoftwaren eller -algoritmen er sårbar, ændres risikoen for fysiske personers rettigheder og frihedsrettigheder, og det kan så være nødvendigt at anmelde bruddet.

Artikel 33 er imidlertid ikke overholdt, når en dataansvarlig undlader at anmelde et brud til tilsynsmyndigheden i en situation, hvor dataene ikke var sikkert krypteret. Når de vælger krypteringssoftware, bør de dataansvarlige derfor omhyggeligt bedømme kvaliteten og den korrekte implementering af den tilbudte kryptering, forstå, hvilket beskyttelsesniveau softwaren rent faktisk giver, og om dette er passende i forhold til de eventuelle risici. De dataansvarlige bør også have kendskab til de nærmere detaljer med hensyn til, hvordan deres krypteringsprodukt fungerer. Udstyr kan f.eks. være krypteret, når det er blevet slukket, men ikke mens det er i standby-mode. Nogle krypteringsprodukter anvender "standardnøgler", der skal ændres af kunderne for at være effektive. Sikkerhedseksperter kan også anse krypteringen for at være passende på krypteringstidspunktet, men den kan blive forældet inden for få år, hvilket sætter spørgsmålstegn ved, om produktet krypterer dataene tilstrækkeligt og sikrer et passende beskyttelsesniveau.

III. **Artikel 34 – Underretning af den registrerede**

A. Underretning af personer

I visse tilfælde skal den dataansvarlige ud over at anmelde et brud til tilsynsmyndigheden også underrette de berørte personer herom.

I artikel 34, stk. 1, bestemmes det, at:

> "Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden.".

De dataansvarlige bør huske på, at anmeldelse til tilsynsmyndigheden er obligatorisk, medmindre det er usandsynligt, at bruddet indebærer en risiko for personers rettigheder og frihedsrettigheder. Når et brud sandsynligvis indebærer en høj risiko for personers rettigheder og frihedsrettigheder, skal de berørte personer også underrettes. Tærsklen for, hvornår de berørte personer skal underrettes om brud, er derfor højere end for, hvornår brud skal anmeldes til tilsynsmyndighederne, og de pågældende personer skal således ikke underrettes om alle brud, hvilket beskytter dem mod unødvendig underretningstræthed.

I GDPR hedder det, at underretning af personer om brud bør ske "uden unødig forsinkelse", dvs. så hurtigt som muligt. Det primære formål med at underrette personer om brud er at give dem specifikke oplysninger om, hvilke forholdsregler de bør træffe for at beskytte sig selv[36]. Som nævnt ovenfor vil rettidig underretning af personer alt efter bruddets art og risikoens alvor hjælpe de berørte personer med at træffe forholdsregler for at beskytte sig selv mod bruddets skadevirkninger.

Bilag B til disse retningslinjer indeholder en ikkeudtømmende liste med eksempler på, hvornår et brud sandsynligvis indebærer en høj risiko for personer, og hvornår den dataansvarlige som følge heraf skal underrette de berørte personer om bruddet.

B. Oplysninger, der skal afgives

Ved underretning af personer fremgår det af artikel 34, stk. 2, at:

> "Underretningen af den registrerede i henhold til denne artikels stk. 1 skal i et klart og forståeligt sprog beskrive karakteren af bruddet på persondatasikkerheden og mindst indeholde de oplysninger og foranstaltninger, der er omhandlet i artikel 33, stk. 3, litra b), c) og d).".

Ifølge denne bestemmelse skal den dataansvarlige mindst afgive følgende oplysninger:

- En beskrivelse af bruddets karakter
- Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt
- En beskrivelse af de sandsynlige konsekvenser af bruddet og
- En beskrivelse af de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger.

[36] Se også betragtning 86.

Som et eksempel på foranstaltninger truffet for at håndtere bruddet og begrænse dets mulige skadevirkninger kan den dataansvarlige oplyse, at denne efter at have anmeldt bruddet til den relevante tilsynsmyndighed har fået råd om håndtering af bruddet og begrænsning af dets konsekvenser. Den dataansvarlige bør også, når dette er relevant, give de berørte personer specifikke råd om, hvordan de kan beskytte sig mod bruddets eventuelle skadevirkninger, herunder ved at nulstille adgangskoder, hvis deres adgangsoplysninger er blevet kompromitteret. Igen kan den dataansvarlige vælge at afgive flere oplysninger end de her påkrævede.

C. Kontakt af personer

I princippet bør de berørte registrerede underrettes om brud direkte, medmindre dette vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde (artikel 34, stk. 3, litra c)).

Der bør anvendes dedikerede meddelelser ved underretning af registrerede om brud, og de bør ikke sendes sammen med andre oplysninger såsom regelmæssige opdateringer, nyhedsbreve eller standardmeddelelser. Dette hjælper med at gøre underretninger om brud klare og gennemsigtige.

Metoder til gennemsigtig underretning kan f.eks. omfatte direct messaging (f.eks. e-mail, SMS, direct message), fremtrædende bannere eller meddelelser på websteder, postforsendelser og fremtrædende reklamer i trykte medier. En underretning, der kun fremgår af en pressemeddelelse eller firmablog, er ikke en effektiv underretning af en person om et brud. Artikel 29-Gruppen anbefaler, at de dataansvarlige vælger et middel, der øger chancen for på behørig vis at formidle oplysninger videre til alle berørte personer. Alt efter forholdene kan dette indebære, at den dataansvarlige anvender flere kommunikationsmidler i modsætning til kun at bruge én kontaktkanal.

De dataansvarlige skal muligvis også sørge for, at underretningen er tilgængelig i passende alternative formater og på relevante sprog for at sikre, at de berørte personer kan forstå de oplysninger, de får forelagt. Ved underretning af en person om et brud er det sprog, der tidligere blev brugt i forretningsforholdet med modtageren, generelt hensigtsmæssigt. Hvis bruddet berører registrerede, som den dataansvarlige endnu ikke har haft kontakt med, eller især registrerede, der bor i en anden medlemsstat eller et andet land uden for EU end det, hvor den dataansvarlige er etableret, kan underretning på det lokale nationale sprog accepteres i betragtning af den påkrævede snarrådighed. Det vigtigste er at hjælpe de registrerede med at forstå karakteren af bruddet og de forholdsregler, de kan træffe for at beskytte sig selv.

De dataansvarlige har de bedste forudsætninger for at afgøre, hvilken kontaktkanal der er bedst egnet til at underrette personer om et brud, især hvis de er i regelmæssig kontakt med deres kunder. Den dataansvarlige skal dog naturligvis være forsigtig med at anvende en kontaktkanal, der er kompromitteret af bruddet, da angriberne også kan anvende denne kanal og give sig ud for at være den dataansvarlige.

På samme tid forklares det i betragtning 86, at:

> "Sådanne underretninger til registrerede bør gives, så snart det med rimelighed er muligt og i tæt samarbejde med tilsynsmyndigheden, i overensstemmelse med retningslinjer, der er udstukket af denne eller af andre relevante myndigheder, såsom de retshåndhævende myndigheder. Eksempelvis kræver behovet for at begrænse en umiddelbar risiko for skade omgående underretning af registrerede, mens behovet for at gennemføre passende foranstaltninger mod fortsatte eller lignende brud på persondatasikkerheden kan begrunde en længere frist for underretning.".

De dataansvarlige kan derfor ønske at kontakte og rådføre sig med tilsynsmyndigheden, for at få råd – ikke kun om underretning af registrerede om et brud i henhold til artikel 34, men også om, hvilke

meddelelser det er bedst at sende til de pågældende personer, og på hvilken måde det er mest hensigtsmæssigt at kontakte dem.

Dette hænger sammen med rådet i betragtning 88 om, at underretning om et brud bør "tage hensyn til de retshåndhævende myndigheders legitime interesser, da en tidlig videregivelse unødigt kan hæmme undersøgelsen af omstændighederne ved et brud på persondatasikkerheden". Dette kan betyde, at den dataansvarlige under visse omstændigheder, når det er berettiget og efter råd fra de retshåndhævende myndigheder, kan udsætte underretningen af de berørte personer om brud, indtil det ikke længere risikerer at skade sådanne undersøgelser. De registrerede skal dog stadig underrettes omgående efter udløbet af et sådant tidsrum.

I det særlige tilfælde, hvor det ikke er muligt for den dataansvarlige at underrette en person om et brud, fordi der er lagret for få oplysninger til, at den pågældende person kan kontaktes, bør den dataansvarlige underrette personen, så snart det med rimelighed er muligt (f.eks. når en person udøver sin ret til adgang til personoplysninger i henhold til artikel 15 og giver den dataansvarlige de supplerende oplysninger, der er nødvendige for, at denne kan kontakte den pågældende).

D. Forhold, hvor underretning ikke er påkrævet

I artikel 34, stk. 3, nævnes tre betingelser, der, hvis de er opfyldt, betyder, at det ikke er nødvendigt at underrette personer om et brud. Der er tale om følgende:

- Den dataansvarlige har gennemført passende tekniske og organisatoriske foranstaltninger til beskyttelse af personoplysninger forud for bruddet, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, f.eks. beskyttelse af personoplysninger med kryptering, som svarer til det aktuelle tekniske niveau, eller tokenisering.
- Umiddelbart efter et brud har den dataansvarlige truffet foranstaltninger, der sikrer, at den høje risiko for de berørte personers rettigheder og frihedsrettigheder sandsynligvis ikke længere er reel. Den dataansvarlige kan f.eks. alt efter sagens omstændigheder omgående have identificeret og iværksat foranstaltninger mod den person, der har fået adgang til personoplysningerne, inden denne nåede at bruge dem til noget. Der skal dog stadig tages højde for de mulige konsekvenser af et brud på fortroligheden, igen alt efter arten af de berørte oplysninger.
- Det vil kræve en uforholdsmæssig indsats[37] at kontakte de berørte personer, måske fordi deres kontaktoplysninger er gået tabt som følge af bruddet, eller fordi de ganske enkelt ikke er kendt. Et statistikkontors lagerbygning er blevet oversvømmet, og dokumenterne, der indeholdt personoplysninger, var kun lagret i papirform. Her skal den dataansvarlige i stedet foretage en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de berørte personer underrettes på en tilsvarende effektiv måde. I tilfælde af en uforholdsmæssig indsats kunne der også overvejes tekniske foranstaltninger, som kunne gøre oplysninger om bruddet tilgængelige på anmodning, hvilket kunne være hensigtsmæssigt for de personer, der er berørt af et brud, men som den dataansvarlige ikke kan kontakte på anden vis.

I overensstemmelse med princippet om ansvarlighed skal de dataansvarlige kunne bevise over for tilsynsmyndigheden, at de overholder en eller flere af disse betingelser [38]. Det bør erindres, at selv om det i første omgang ikke er nødvendigt at anmelde et brud, hvis det ikke indebærer en risiko for

[37] Se Artikel 29-Gruppens retningslinjer om gennemsigtighed, som ser på spørgsmålet om uforholdsmæssig indsats, på http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850.

[38] Se artikel 5, stk. 2.

fysiske personers rettigheder og frihedsrettigheder, kan dette ændre sig med tiden, hvorefter risikoen skal evalueres på ny.

Hvis en dataansvarlig beslutter sig for ikke at underrette personer om et brud, forklares det i artikel 34, stk. 4, at tilsynsmyndigheden kan kræve, at den dataansvarlige gør dette, hvis den mener, at bruddet sandsynligvis indebærer en høj risiko for de pågældende personer. Alternativt kan tilsynsmyndigheden beslutte, at betingelserne i artikel 34, stk. 3, er opfyldt, og at det dermed ikke er nødvendigt at underrette dem. Hvis tilsynsmyndigheden beslutter, at afgørelsen om ikke at underrette de registrerede er uberettiget, kan den overveje at udøve sine beføjelser og pålægge sanktioner.

IV. **Vurdering af risiko og høj risiko**

A. Risiko som en udløser for anmeldelse

Selv om GDPR indfører forpligtelsen til at anmelde brud, er det ikke et krav, at dette gøres i alle tilfælde.

- Anmeldelse til den kompetente tilsynsmyndighed er påkrævet, medmindre bruddet sandsynligvis ikke indebærer en risiko for personers rettigheder eller frihedsrettigheder.
- Kravet om underretning af personer om et brud udløses først, når bruddet sandsynligvis indebærer en høj risiko for deres rettigheder og frihedsrettigheder.

Det betyder, at det er af afgørende betydning, at den dataansvarlige, så snart denne bliver bekendt med et brud, ikke blot forsøger at inddæmme hændelsen, men også vurderer den risiko, som hændelsen indebærer. Det er der to væsentlige grunde til. For det første hjælper viden om sandsynligheden for og den potentielle alvor af et bruds virkning for personer den dataansvarlige med at træffe effektive forholdsregler for at inddæmme og håndtere bruddet. For det andet hjælper det den dataansvarlige med at beslutte, om anmeldelse til tilsynsmyndigheden og eventuelt til de berørte personer er påkrævet.

Som forklaret ovenfor er anmeldelse af et brud påkrævet, medmindre bruddet sandsynligvis ikke indebærer en risiko for personers rettigheder eller frihedsrettigheder, og kravet om underretning af de registrerede om et brud udløses, når bruddet sandsynligvis indebærer en *høj* risiko for de registreredes rettigheder og frihedsrettigheder. Denne risiko foreligger, når bruddet kan medføre fysisk, materiel eller immateriel skade på de personer, hvis data er omfattet af bruddet. Eksempler på sådan skade er forskelsbehandling, identitetstyveri eller -svig, finansielle tab og skade på omdømme. Hvis bruddet involverer personoplysninger, der viser race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, eller omfatter genetiske data, helbredsoplysninger eller oplysninger om seksuelle forhold eller straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger, bør en sådan skade opfattes som værende sandsynlig[39].

B. Faktorer, der skal tages i betragtning ved risikovurdering

Af betragtning 75 og 76 i GDPR fremgår det, at der generelt ved risikovurderingen bør tages hensyn til såvel risikoens sandsynlighed som dens alvor for så vidt angår den registreredes rettigheder og frihedsrettigheder. Det fremgår endvidere, at risikoen bør evalueres på grundlag af en objektiv vurdering.

[39] Se betragtning 75 og 85.

Det skal bemærkes, at der ved vurdering af den risiko for folks rettigheder og frihedsrettigheder, som et brud indebærer, fokuseres på noget andet end i en konsekvensanalyse vedrørende databeskyttelse[40]. Konsekvensanalysen vedrørende databeskyttelse omhandler både de risici, der er forbundet med den planlagte databehandling, og de risici, der opstår i tilfælde af brud. Med hensyn til potentielle brud ses der mere overordnet på sandsynligheden for, at et brud opstår, og den skade, et sådant brud kunne påføre den registrerede. Det er med andre ord en vurdering af en hypotetisk hændelse. Ved et faktisk brud er hændelsen allerede opstået, så der fokuseres udelukkende på den risiko, som bruddet indebærer for de berørte personer.

Eksempel

Af en konsekvensanalyse vedrørende databeskyttelse fremgår det, at den foreslåede anvendelse af en bestemt sikkerhedssoftware er en passende foranstaltning til sikring af et sikkerhedsniveau, der står i et rimeligt forhold til den risiko, behandlingen ellers ville indebære for de berørte personer. Hvis man efterfølgende får kendskab til en sårbarhed, ændrer det imidlertid softwarens egnethed til at inddæmme risikoen for de beskyttede personoplysninger, og den skal vurderes på ny som led i en løbende konsekvensanalyse vedrørende databeskyttelse.

Senere bliver en sårbarhed i produktet udnyttet, og der opstår et brud. Den dataansvarlige bør vurdere de specifikke omstændigheder omkring bruddet, de berørte data og den potentielle virkning for de berørte personer, samt hvor stor sandsynligheden er for, at risikoen bliver reel.

Tilsvarende bør den dataansvarlige ved vurdering af den risiko, som et brud indebærer for personer, tage hensyn til de specifikke forhold omkring bruddet, herunder konsekvensernes potentielle alvor og sandsynligheden for, at de opstår. Artikel 29-Gruppen anbefaler derfor, at der ved vurderingen tages hensyn til følgende kriterier[41]:

- Bruddets type

Typen af det brud, der er opstået, kan have betydning for den dermed forbundne risiko for de berørte personer. Et brud på fortroligheden, hvor helbredsoplysninger er blevet offentliggjort for uautoriserede parter, kan f.eks. have andre konsekvenser for en person end et brud, hvor en persons helbredsoplysninger er blevet tabt og ikke længere er tilgængelige.

- Personoplysningernes art, følsomhed og mængde

Ved vurdering af en risiko er typen og følsomheden af de personoplysninger, der er kompromitteret af bruddet, naturligvis en central faktor. Jo mere følsomme oplysningerne er, jo større er risikoen normalt for skade på de berørte personer, men der bør også tages hensyn til andre personoplysninger om de registrerede, der måske allerede er tilgængelige. F.eks. er det usandsynligt, at offentliggørelse af en persons navn og adresse under normale omstændigheder vil påføre den pågældende omfattende skade. Men hvis en adoptivforælders navn og adresse offentliggøres for en biologisk forælder, kan konsekvenserne være særdeles alvorlige for både adoptivforælderen og barnet.

[40] Se gruppens retningslinjer om konsekvensanalyser vedrørende databeskyttelse her: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[41] Artikel 3, stk. 2, i forordning 611/2013 indeholder en vejledning om de faktorer, der bør tages hensyn til i forbindelse med underretning om brud i den elektroniske kommunikationssektor, som kan være praktisk i forbindelse med anmeldelse i henhold til GDPR. Se http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:da:PDF.

Brud, der vedrører helbredsoplysninger, identitetspapirer eller finansielle oplysninger såsom kreditkortoplysninger, kan påføre skade hver for sig, men hvis oplysningerne anvendes sammen, kan de bruges til identitetstyveri. En kombination af personoplysninger er typisk mere følsom end en enkelt personoplysning.

Nogle typer personoplysninger kan forekomme ganske harmløse, men det skal overvejes nøje, hvad disse oplysninger kan afsløre om den pågældende person. En liste over kunder, der får leveret varer regelmæssigt, er måske ikke særlig følsom, men de samme oplysninger om kunder, der har anmodet om at få indstillet leveringerne, mens de er på ferie, er nyttige oplysninger for kriminelle.

Tilsvarende kan en lille mængde særdeles følsomme personoplysninger have stor virkning for en person, mens en stor mængde forskellige oplysninger kan afsløre endnu flere oplysninger om personen. Et brud, der berører store mængder personoplysninger om mange registrerede, kan have virkning for et tilsvarende stort antal personer.

- Nem identificering af personer

En vigtig faktor, der skal tages i betragtning, er, hvor nemt det er for en part, der har adgang til kompromitterede personoplysninger, at identificere specifikke personer eller matche oplysningerne med andre oplysninger for at identificere personer. Alt efter forholdene kan det være muligt at identificere en person direkte ud fra de personoplysninger, der er omfattet af bruddet, uden at det er nødvendigt at foretage særlige undersøgelser for at afsløre personens identitet, eller det kan være ekstremt vanskeligt at matche personoplysninger med en bestemt person, men dog stadig muligt under visse omstændigheder. Identificering kan være mulig direkte eller indirekte ud fra de data, der er omfattet af et brud, men det kan også afhænge af de specifikke forhold omkring bruddet og offentlighedens adgang til relaterede personoplysninger. Dette er formodentlig mest relevant i forbindelse med brud på fortrolighed og tilgængelighed.

Som nævnt ovenfor er personoplysninger, som er beskyttet af et passende krypteringsniveau, uforståelige for uautoriserede personer uden dekrypteringskoden. Derudover kan korrekt implementeret pseudonymisering (defineret i artikel 4, stk. 5, som "behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person") også mindske sandsynligheden for, at personer kan identificeres i tilfælde af brud. Pseudonymiseringsteknikker kan dog ikke alene anses for at gøre data uforståelige.

- Konsekvensernes alvor for personer

Alt efter arten af de personoplysninger, der er involveret i et brud, f.eks. særlige kategorier af personoplysninger, kan den dermed forbundne potentielle skade for personer være særdeles alvorlig, navnlig når bruddet kan resultere i identitetstyveri eller -svig, fysisk eller psykisk skade, ydmygelse eller skade på omdømme. Hvis bruddet vedrører personoplysninger om sårbare personer, kan risikoen for skade være endnu større.

Om den dataansvarlige er bekendt med, at folk med ukendte eller muligvis ondsindede intentioner er kommet i besiddelse af personoplysninger, kan have betydning for det potentielle risikoniveau. Der kan være sket et brud på fortroligheden, hvorved personoplysninger fejlagtigt er blevet offentliggjort for tredjemand, jf. artikel 4, stk. 10, eller en anden modtager. Dette kan f.eks. ske, når personoplysninger utilsigtet sendes til den forkerte afdeling i en organisation eller til en ofte anvendt forsyningsorganisation. Den dataansvarlige kan anmode modtageren om enten at tilbagelevere eller sikkert destruere de modtagne data. I begge tilfælde kan modtageren opfattes som betroet, eftersom den dataansvarlige løbende har kontakt til dem og eventuelt er bekendt med deres procedurer, historie og andre relevante oplysninger. Den dataansvarlige kan med andre ord have et tillidsforhold til

modtageren, så han eller hun med rimelighed kan forvente, at den pågældende ikke læser eller forsøger at få adgang til de fejlagtigt fremsendte data og efterlever den dataansvarliges instrukser om at levere dem tilbage. Selv om modtageren har fået adgang til dataene, kan den dataansvarlige formentlig alligevel have tillid til, at modtageren ikke vil bruge dem til noget og omgående vil levere dem tilbage til den dataansvarlige og samarbejde med denne om at få dem bragt tilbage. I sådanne tilfælde kan der tages hensyn hertil i den risikovurdering, som den dataansvarlige foretager efter bruddet – det forhold, at modtageren er betroet, kan minimere alvoren af bruddets konsekvenser, men betyder ikke, at der ikke er sket et brud. Det kan til gengæld fjerne sandsynligheden for, at bruddet indebærer en risiko for personer, og det er derfor ikke længere nødvendigt at anmelde bruddet til tilsynsmyndigheden eller underrette de berørte personer herom. Igen afhænger dette af hver enkelt sag. Ikke desto mindre skal den dataansvarlige stadig gemme oplysninger om bruddet som led i den generelle forpligtelse til at føre fortegnelser over brud (se afsnit V nedenfor).

Der bør også tages hensyn til konsekvensernes varighed for de berørte personer, hvor virkningen kan ses som større, hvis konsekvenserne er langvarige.

- Personens særlige karakteristika

Et brud kan vedrøre personoplysninger om børn eller andre sårbare personer, som derfor er i større fare for at blive skadet af bruddet. Der kan også være andre forhold omkring en person, der har betydning for bruddets indvirkning på personen.

- Den dataansvarliges særlige karakteristika

Den dataansvarliges art og rolle samt aktiviteter kan have betydning for den risiko, et brud indebærer for en person. En sundhedsorganisation behandler f.eks. særlige kategorier af personoplysninger, hvilket indebærer en større risiko for de berørte personer, hvis deres personoplysninger bliver involveret i et brud, sammenlignet med personer på en avis' mailingliste.

- Antal berørte personer

Et brud kan påvirke én eller få eller flere tusinde personer eller mange flere. Generelt gælder det, at jo flere personer der er berørt af et brud, jo større virkning kan bruddet have. Et brud kan dog også have en alvorlig virkning for bare én person alt efter arten af personoplysningerne og den sammenhæng, inden for hvilken oplysningerne er blevet kompromitteret. Igen er det centrale at tage højde for virkningens sandsynlighed og alvor for de berørte personer.

- Generelt

Derfor skal den dataansvarlige, når denne vurderer den risiko, et brud sandsynligvis indebærer, overveje en kombination af alvoren af den potentielle virkning for personers rettigheder og frihedsrettigheder og sandsynligheden for, at denne virkning opstår. Det er klart, at når konsekvenserne af et brud er alvorlige, er risikoen højere, og tilsvarende når sandsynligheden for, at konsekvenserne opstår, er stor, er risikoen også højere. Hvis den dataansvarlige er i tvivl, bør denne vælge den sikre løsning og underrette de berørte parter. Bilag B indeholder nyttige eksempler på forskellige typer brud, som indebærer en risiko eller en høj risiko for personer.

Den Europæiske Unions Agentur for Net- og Informationssikkerhed (ENISA) har fremsat anbefalinger til en metode for vurdering af alvoren af et brud, som de dataansvarlige og databehandlerne kan finde nyttige, når de udarbejder deres beredskabsplan for håndtering af brud[42].

V. Ansvarlighed og fortegnelser

A. Dokumentation af brud

Uanset om et brud skal anmeldes til tilsynsmyndigheden eller ej, skal den dataansvarlige dokumentere bruddet, jf. artikel 33, stk. 5:

> "Den dataansvarlige dokumenterer alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at denne artikel er overholdt."

Dette hænger sammen med princippet om ansvarlighed i GDPR, som fremgår af artikel 5, stk. 2. Formålet med at føre fortegnelser over brud, der ikke skal anmeldes, og brud, der skal anmeldes, er også knyttet til den dataansvarliges forpligtelser i artikel 24, og tilsynsmyndigheden kan kræve at se disse fortegnelser. De dataansvarlige opfordres derfor til at føre et internt register over brud, uanset om bruddene skal anmeldes eller ej[43].

Mens det er op til den dataansvarlige at afgøre, hvilken metode og struktur der skal anvendes til dokumentation af brud, er der med hensyn til de registrerede oplysninger centrale elementer, der altid skal medtages. I henhold til artikel 33, stk. 5, skal den dataansvarlige føre fortegnelser over oplysninger om bruddet, som skal omfatte årsagerne til bruddet, hvad der skete, og hvilke personoplysninger der er berørt af bruddet. Derudover skal bruddets virkninger og konsekvenser registreres sammen med de afhjælpende foranstaltninger, den dataansvarlige har truffet.

GDPR fastsætter ikke en bestemt opbevaringsperiode for sådan dokumentation. Når fortegnelserne indeholder personoplysninger, påhviler det den dataansvarlige at fastsætte en passende opbevaringsperiode i overensstemmelse med principperne for behandling af personoplysninger[44] og opfylde kravene om lovlig behandling[45]. Den dataansvarlige skal opbevare dokumentationen i henhold til artikel 33, stk. 5, og skal kunne dokumentere over for tilsynsmyndigheden, at artiklen – eller princippet om ansvarlighed generelt – er overholdt. Hvis fortegnelserne selv ikke indeholder personoplysninger, finder princippet om opbevaringsbegrænsning[46] i GDPR naturligvis ikke anvendelse.

---

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches (anbefalinger til en metode for vurdering af alvoren af brud på persondatasikkerheden), https://www.enisa.europa.eu/publications/dbn-severity.

[43] Den dataansvarlige kan vælge at dokumentere brud i sine fortegnelser over behandlingsaktiviteter, der føres i henhold til artikel 30. Det er ikke påkrævet at føre et separat register, så længe oplysningerne om brud klart kan identificeres som sådanne og kan trækkes ud på anmodning.

[44] Se artikel 5.

[45] Se artikel 6 og artikel 9.

[46] Se artikel 5, stk. 1, litra e).

Herudover anbefaler Artikel 29-Gruppen, at den dataansvarlige også dokumenterer sin begrundelse for de beslutninger, der træffes i forbindelse med brud. Især bør begrundelsen for en beslutning om ikke at anmelde et brud dokumenteres. Dette omfatter grundene til, at den dataansvarlige mener, at bruddet sandsynligvis ikke indebærer en risiko for personers rettigheder eller frihedsrettigheder[47]. Hvis den dataansvarlige mener, at en eller flere af betingelserne i artikel 34, stk. 3, er opfyldt, bør denne alternativt kunne bevise, at dette er tilfældet.

Hvis den dataansvarlige anmelder et brud til tilsynsmyndigheden, men anmeldelsen er forsinket, skal den dataansvarlige kunne begrunde forsinkelsen. Dokumentation herom kan hjælpe med at påvise, at rapporteringsforsinkelsen er berettiget og ikke urimelig.

Når den dataansvarlige underretter de berørte personer om et brud, bør han eller hun være åben om bruddet og underrette dem effektivt og rettidigt. Tilsvarende vil det hjælpe den dataansvarlige med at bevise sin ansvarlighed og opfyldelse af sine forpligtelser, hvis han gemmer beviser for denne underretning.

For at bidrage til overholdelsen af artikel 33 og 34 ville det være fordelagtigt for såvel dataansvarlige som databehandlere at indføre en dokumenteret anmeldelsesprocedure, som fastlægger den fremgangsmåde, der skal følges, når et brud er detekteret, herunder hvordan hændelsen skal inddæmmes, håndteres og afhjælpes, samt ved risikovurdering og anmeldelse af bruddet. I denne forbindelse kan det for at vise, at GDPR er overholdt, også være hensigtsmæssigt at påvise, at personalet er blevet underrettet om, at sådanne procedurer og mekanismer findes, og at de ved, hvordan de skal reagere på brud.

Det skal bemærkes, at manglende korrekt dokumentation af et brud kan få tilsynsmyndigheden til at udøve sine beføjelser i henhold til artikel 58 og/eller pålægge en administrativ bøde i henhold til artikel 83.

B. Databeskyttelsesrådgiverens rolle

En dataansvarlig eller databehandler kan have en databeskyttelsesrådgiver[48]. Det kan enten være obligatorisk, jf. artikel 37, eller frivilligt som led i god praksis. Artikel 39 i GDPR indeholder en række opgaver, der er obligatoriske for databeskyttelsesrådgiveren, men forhindrer ikke, at den dataansvarlige eventuelt betror databeskyttelsesrådgiveren yderligere opgaver.

I forbindelse med anmeldelse af brud omfatter databeskyttelsesrådgiverens obligatoriske opgaver bl.a. rådgivning og oplysning af den dataansvarlige og databehandleren om databeskyttelse, overvågning af overholdelsen af GDPR og rådgivning med hensyn til konsekvensanalysen vedrørende databeskyttelse. Databeskyttelsesrådgiveren skal endvidere samarbejde med tilsynsmyndigheden og fungere som kontaktpunkt for tilsynsmyndigheden og de registrerede. Det skal desuden bemærkes, at den dataansvarlige ved anmeldelse af et brud til tilsynsmyndigheden i henhold til artikel 33, stk. 3, litra b), skal angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt.

Med hensyn til dokumentation af brud kan den dataansvarlige eller databehandleren bede databeskyttelsesrådgiveren om dennes mening om f.eks. dokumentationens struktur, opsætning og forvaltning. Databeskyttelsesrådgiveren kan også få til opgave at føre sådanne fortegnelser.

---

[47] Se betragtning 85.

[48] Se gruppens retningslinjer om databeskyttelsesrådgivere her: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Det betyder, at databeskyttelsesrådgiveren bør spille en central rolle og bidrage til forebyggelse af eller forberedelse på et brud ved at rådgive og overvåge overholdelsen af GDPR, både mens et brud står på (f.eks. ved anmeldelse til tilsynsmyndigheden) og under tilsynsmyndighedens efterfølgende undersøgelse. På denne baggrund anbefaler Artikel 29-Gruppen, at databeskyttelsesrådgiveren omgående underrettes om et brud og inddrages i hele processen med håndtering og anmeldelse af bruddet.

VI. Anmeldelsespligt i henhold til andre retsakter

Ud over og adskilt fra kravene om anmeldelse af og underretning om brud i GDPR bør de dataansvarlige også være opmærksomme på andre krav om anmeldelse af sikkerhedshændelser i anden tilknyttet lovgivning, der måtte finde anvendelse på dem, og på, om denne også samtidig forpligter dem til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden. Disse krav kan variere medlemsstaterne imellem, men nedenfor findes en række eksempler på anmeldelseskrav i andre retsakter og på, hvordan disse hænger sammen med GDPR:

- Forordning (EU) nr. 910/2014 om elektronisk identifikation og tillidstjenester til brug for elektroniske transaktioner på det indre marked (eIDAS-forordningen)[49]

I henhold til artikel 19, stk. 2, i eIDAS-forordningen skal tillidstjenesteudbydere underrette tilsynsorganet om brud på sikkerheden eller tab af integritet, som har en væsentlig indvirkning på den udbudte tillidstjeneste eller de berørte personoplysninger. Når det er relevant – dvs. når et sådant brud eller tab også udgør et brud på persondatasikkerheden i henhold til GDPR – skal tillidstjenesteudbyderen også underrette tilsynsmyndigheden.

- Direktiv (EU) 2016/1148 om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet)[50]

Artikel 14 og 16 i NIS-direktivet kræver, at operatører af væsentlige tjenester og digitale tjenester underretter den kompetente myndighed om sikkerhedshændelser. Som der står i betragtning 63 i NIS[51], bliver personoplysninger i mange tilfælde kompromitteret som følge af sikkerhedshændelser. Mens NIS kræver, at de kompetente myndigheder og tilsynsmyndighederne samarbejder og udveksler oplysninger om alle relevante spørgsmål, er det fortsat sådan, at når disse hændelser er – eller bliver til – brud på persondatasikkerheden i henhold til GDPR, skal disse operatører og/eller udbydere også underrette tilsynsmyndigheden ud over at overholde kravene om underretning om hændelser i NIS.

Eksempel

En cloud-tjenesteudbyder, der underretter om et brud i henhold til NIS-direktivet, skal også underrette en dataansvarlig, hvis bruddet omfatter et brud på persondatasikkerheden. Tilsvarende skal en tillidstjenesteudbyder, som underretter om et brud i henhold til eIDAS, også underrette den relevante databeskyttelsesmyndighed.

[49] Se http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.DAN.

[50] Se http://eur-lex.europa.eu/legal-content/DA/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.DAN.

51 Betragtning 63: *"Personoplysninger er i mange tilfælde kompromitteret som følge af hændelser. De kompetente myndigheder og databeskyttelsesmyndighederne bør i denne forbindelse samarbejde og udveksle oplysninger om alle relevante spørgsmål for at håndtere alle brud på persondatasikkerheden som følge af hændelser."*

- Direktiv 2009/136/EF (borgerrettighedsdirektivet) og forordning 611/2013 (forordningen om underretning om brud)

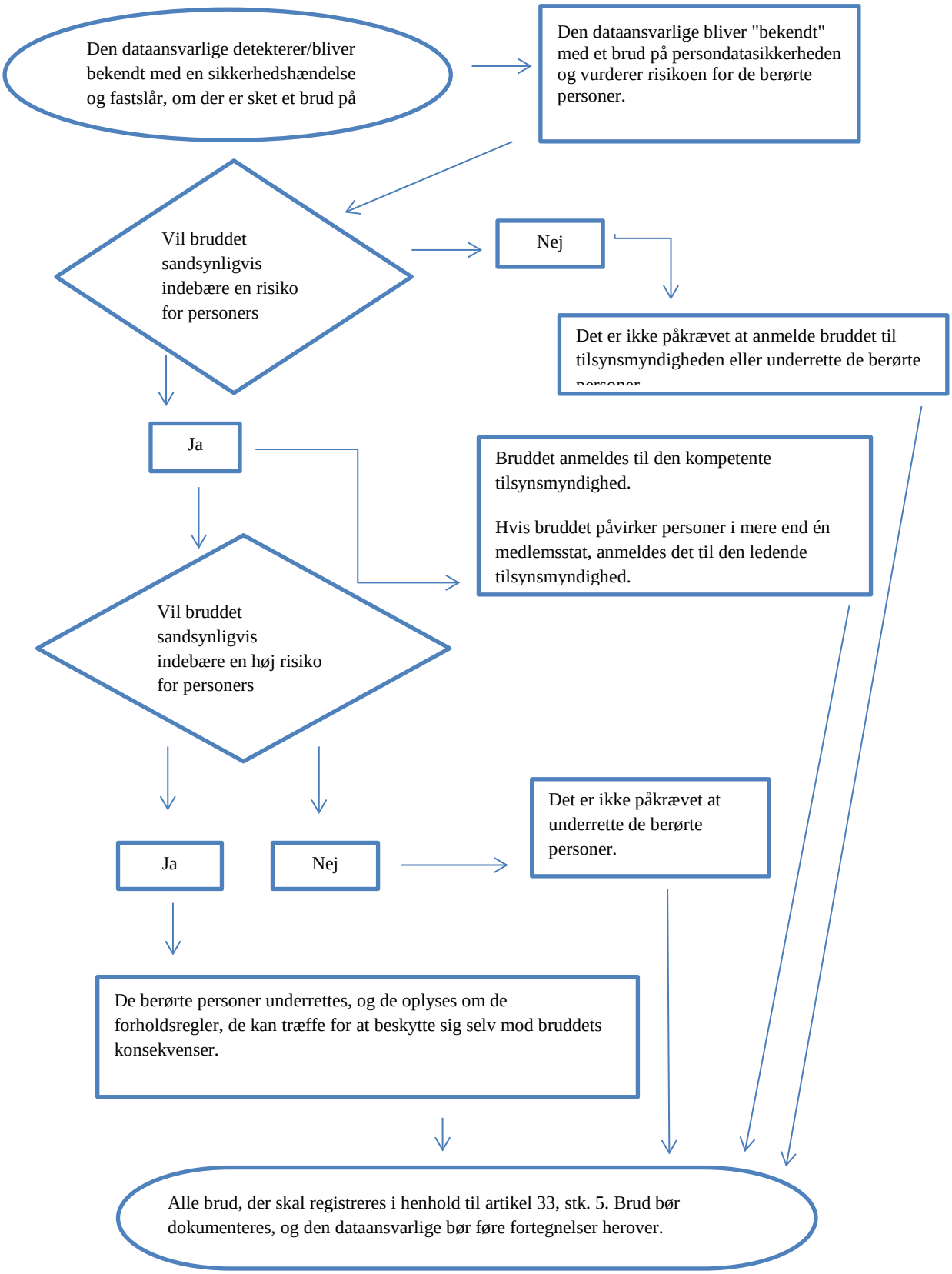
Udbydere af offentligt tilgængelige elektroniske kommunikationstjenester i henhold til direktiv 2002/58/EF[52] skal underrette de kompetente nationale myndigheder om brud.

De dataansvarlige skal endvidere være opmærksomme på eventuelle supplerende juridiske, medicinske eller erhvervsmæssige forpligtelser i henhold til andre gældende ordninger.

[52] Den 10.1.2017 fremsatte Europa-Kommissionen et forslag til forordning om respekt for privatliv og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation, som vil erstatte direktiv 2009/136/EF og afskaffe kravet om underretning. Indtil forslaget er blevet godkendt af Europa-Parlamentet, gælder det eksisterende krav om underretning imidlertid fortsat, se https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

VII. **Bilag**

A. Flowdiagram over anmeldelseskrav



B. Eksempler på brud på persondatasikkerheden og på, hvem der skal underrettes

Følgende ikkeudtømmende liste med eksempler hjælper de dataansvarlige med at fastslå, om de skal anmelde et brud inden for forskellige scenarier for brud på persondatasikkerheden. Eksemplerne kan også hjælpe med at skelne mellem risiko og høj risiko for personers rettigheder og frihedsrettigheder.

Eksempel	**Skal bruddet anmeldes til tilsynsmyndigheden?**	**Skal den registrerede underrettes?**	**Bemærkninger/anbefalinger**
i. En dataansvarlig har gemt en backup af et bibliotek med personoplysninger krypteret på en USB-nøgle. Nøglen bliver stjålet under et indbrud.	Nej.	Nej.	Så længe dataene er krypteret med en algoritme, som svarer til det aktuelle tekniske niveau, der findes en backup af dataene, den unikke nøgle ikke er kompromitteret, og dataene kan gendannes rettidigt, udgør dette ikke nødvendigvis et brud, der skal rapporteres. Hvis dataene senere bliver kompromitteret, skal bruddet anmeldes.
ii. En dataansvarlig har en onlinetjeneste. Som følge af et cyberangreb på tjenesten bliver personoplysninger eksfiltreret. Den dataansvarlige har kunder i en enkelt medlemsstat.	Ja, bruddet skal rapporteres til tilsynsmyndigheden, hvis det sandsynligvis har konsekvenser for de berørte personer.	Ja, bruddet skal rapporteres til de berørte personer alt efter arten af de pågældende personoplysninger, og hvis de sandsynlige konsekvenser for de berørte personer er alvorlige.	
iii. En kort strømafbrydelse på nogle minutter på en dataansvarligs call-center betyder, at kunderne ikke kan ringe til den dataansvarlige og få adgang til deres oplysninger.	Nej.	Nej.	Dette brud skal ikke anmeldes, men er stadig en hændelse, som skal registreres i henhold til artikel 33, stk. 5. Den dataansvarlige bør føre relevante fortegnelser.
iv. En dataansvarlig bliver udsat for et ransomware-angreb, som resulterer i, at alle data bliver krypteret. Der findes ingen	Ja, bruddet skal rapporteres til tilsynsmyndigheden, hvis det sandsynligvis har konsekvenser for de berørte personer,	Ja, bruddet skal rapporteres til de berørte personer alt efter arten af de pågældende personoplysninger	Hvis der fandtes en backup, og dataene kunne gendannes rettidigt, ville det ikke være nødvendigt at rapportere bruddet til tilsynsmyndigheden eller de

backup, og dataene kan ikke gendannes. Efter en undersøgelse bliver det fastslået, at ransomwarens eneste funktion var at kryptere dataene, og at der ikke var anden malware i systemet.	da der er tale om et tab af tilgængelighed.	og den mulige virkning af dataenes manglende tilgængelighed samt andre sandsynlige konsekvenser.	berørte personer, da der ikke ville være sket et varigt tab af tilgængelighed eller fortrolighed. Hvis tilsynsmyndigheden bliver bekendt med hændelsen ad anden vej, kan den dog overveje at indlede en undersøgelse for at vurdere overholdelsen af de generelle sikkerhedskrav i artikel 32.
v. En person ringer til en banks call-center for at rapportere et brud på datasikkerheden. Personen har modtaget en anden kundes kontoudskrift. Den dataansvarlige foretager en kort undersøgelse (som afsluttes inden for 24 timer) og fastslår med rimelig sikkerhed, at der er sket et brud på persondatasikkerheden, og om der er opstået en systemisk fejl, der betyder, at andre personer er eller muligvis bliver berørt.	Ja.	Kun de berørte personer underrettes, hvis der er en høj risiko, og det er sikkert, at andre ikke er berørt.	Hvis det efter yderligere undersøgelser slås fast, at flere andre er berørt, sendes en opdatering til tilsynsmyndigheden, og den dataansvarlige iværksætter yderligere foranstaltninger for at underrette de øvrige personer, hvis der er en høj risiko for dem.
vi. En dataansvarlig driver en online markedsplads og har kunder i flere medlemsstater. Markedspladsen udsættes for et cyberangreb, og angriberen offentliggør brugernavne, adgangskoder og købshistorik online.	Ja, bruddet skal rapporteres til den ledende tilsynsmyndighed, hvis der er tale om grænseoverskridende behandling.	Ja, da det kan indebære en høj risiko.	Den dataansvarlige skal gribe ind, f.eks. ved at gennemtvinge en nulstilling af adgangskoderne til de berørte konti, og iværksætte yderligere foranstaltninger for at afbøde risikoen. Den dataansvarlige skal også tage højde for andre forpligtelser til at anmelde bruddet, f.eks. i NIS-direktivet som udbyder af en digital tjeneste.
vii. Et webhosting-selskab, der fungerer som databehandler,	Som databehandler skal webhosting-selskabet underrette	Hvis der sandsynligvis ikke er en høj risiko for	Webhosting-selskabet (databehandleren) skal tage højde for andre forpligtelser

identificerer en fejl i den kode, som styrer brugergodkendelsen. Fejlen betyder, at alle brugere kan få adgang til alle de andre brugeres kontooplysninger.	de berørte klienter (de dataansvarlige) uden unødig forsinkelse. Under forudsætning af at webhosting-selskabet har foretaget egne undersøgelser, bør de berørte dataansvarlige med rimelig sikkerhed vide, om de har været udsat for et brud, og kan derfor sandsynligvis opfattes som værende "bekendt" med hændelsen, når de er blevet underrettet af hosting-selskabet (databehandleren). Den dataansvarlige anmelder så efterfølgende bruddet til tilsynsmyndigheden.	de berørte personer, er det ikke nødvendigt at underrette dem.	til at anmelde bruddet (f.eks. i NIS-direktivet som udbyder af en digital tjeneste). Hvis der ikke foreligger bevis for, at sårbarheden er blevet udnyttet hos nogen af de dataansvarlige, er der ikke nødvendigvis sket et brud, der skal anmeldes, men det skal sandsynligvis registreres eller kan være omfattet af bestemmelserne om manglende overholdelse i artikel 32.
viii. På et hospital er lægejournalerne utilgængelige i 30 timer som følge af et cyberangreb.	Ja, hospitalet er forpligtet til at anmelde bruddet, da der kan være høj risiko for patienternes velbefindende og ret til privatliv.	Ja, skal rapporteres til de berørte personer.	
ix. Personoplysninger om et stort antal studerende er ved en fejl blevet sendt til den forkerte mailingliste med over 1 000 modtagere.	Ja, skal rapporteres til tilsynsmyndigheden.	Ja, skal rapporteres til de berørte personer alt efter omfanget og typen af de berørte personoplysninger og de eventuelle konsekvensers alvor.	
x. En direkte markedsførings-e-mail sendes til modtagerne i feltet "til" eller "cc.", hvorved modtagerne kan se de øvrige	Ja, det kan være nødvendigt at anmelde det til tilsynsmyndigheden, hvis et stort antal personer er berørt,	Ja, skal rapporteres til de berørte personer alt efter omfanget og typen af de berørte	Det kan være unødvendigt at anmelde bruddet, hvis ikke der afsløres følsomme oplysninger, og hvis det kun er et mindre antal e-mail-adresser, der afsløres.

modtageres e-mail-adresser.	hvis der afsløres følsomme oplysninger (f.eks. en psykoterapeuts mailingliste), eller hvis andre faktorer indebærer en høj risiko (hvis f.eks. mailen indeholder de oprindelige adgangskoder).	personoplysninger og de eventuelle konsekvensers alvor.	