Håndtering af brud på persondatasikkerheden

Vejledning

Maj 2025

DATATILSYNET

Ændringslog

Dato	Ændring/opdatering
14. maj 2025	Opdatering af hele vejledningen, herunder indhold, layout, eksempler og henvisninger.

Indhold

1. Forord 5

2. Hvornår er der sket et brud på persondatasikkerheden 6

2.1 Definition på et brud på persondatasikkerheden 6

2.2 Informationssikkerhedsrisici og brud på persondatasikkerheden 8

2.3 Eksempler på brud 8

Eksempel 1: Flytbart medie bliver stjålet **9**
Eksempel 2: Oplysningerne mistes **9**
Eksempel 3: Hacker får adgang til oplysninger **10**
Eksempel 4: Hacker prøver at få adgang **10**
Eksempel 5: Sårbarhed i firewall **11**
Eksempel 6: Ramt af ransomware **12**
Eksempel 7: Papirer med oplysninger bliver stjålet **12**
Eksempel 8: Vandskade på server **13**
Eksempel 9: Nedbrud i system **13**
Eksempel 10: Planlagt nedetid **13**
Eksempel 11: Medarbejder videregiver oplysninger ulovligt **13**
Eksempel 12: Oplysninger til forkert modtager **14**
Eksempel 13: Uautoriseret adgang **14**
Eksempel 14: Utilsigtet offentliggørelse **16**
Eksempel 15: Transmission uden kryptering **16**
Eksempel 16: Fejl i systemintegration **16**
Eksempel 17: Fejl ved alarmknap **17**

3. Anmeldelse til Datatilsynet 18

3.1 Hvordan foretages anmeldelse til Datatilsynet? 18

3.2 Hvilke brud på persondatasikkerheden kræver anmeldelse? 18

3.2.1 Typen af brud 19
3.2.2 Kategorier og mængden af oplysninger 19
3.2.3 Muligheden for at identificere personer 20
3.2.4 Mulige konsekvenser for de berørte personer 20
3.2.5 Hvem, der eventuelt har fået uretmæssig adgang til personoplysningerne 21
3.2.6 Bruddets varighed 21
3.2.7 Særligt sårbare registrerede 21
3.2.8 Antallet af berørte personer 22

3.3 Tidspunktet for anmeldelse 22

3.3.1 Bekendt med bruddet 22
3.3.2 Uden unødig forsinkelse 23

3.4 Hvem skal anmelde til Datatilsynet? 24

3.5 Hvilke forpligtelser har databehandleren? 24

3.6 Hvilke oplysninger skal gives til Datatilsynet? 25

3.7 Situationer, hvor anmeldelse til Datatilsynet ikke er nødvendigt 25

3.8 Eksempler 26

3.9 Hvis bruddet indebærer en risiko for registrerede i flere lande 26
Eksempel 18: Tilsynsmyndighed 27
4. Underretning af den registrerede 28
4.1 Hvilke brud på persondatasikkerheden kræver underretning? 28
4.2 Hvornår skal underretning ske? 28
4.3 Hvilke oplysninger skal indgå i en underretning? 29
4.3.1 Kontaktoplysninger 29
4.3.2 Beskrivelse af karakteren af bruddet i et klart og forståeligt sprog 29
4.3.3 Beskrivelse af sandsynlige konsekvenser 30
4.3.4 Beskrivelse af foranstaltninger 31
4.3.5 Anbefalinger og specifikke råd til den registrerede 31
4.3.6 Opfølgende underretning 32
4.4 Hvordan skal den registrerede underrettes 32
4.5 Hvem kan foretage underretning af de registrerede 32
4.6 Situationer, hvor der ikke er krav om underretning 33
4.6.1 Foranstaltninger før bruddet reducerer risikoen 33
4.6.2 Foranstaltninger efter bruddet reducerer risikoen 33
4.6.3 Underretning kræver en uforholdsmæssig indsats 33
4.6.4 Underretning kan undlades i henhold til national lovgivning 34
4.7 Eksempler 34
4.8 Underretning efter krav fra Datatilsynet 35
5. Ansvarlighed og intern dokumentation 36
6. Krav om anmeldelse til andre myndigheder i medfør af anden lovgivning 38
6.1 Digitaliseringsstyrelsen 38
6.2 Styrelsen for Samfundssikkerhed 38
6.3 Finanstilsynet 38
6.4 NIS2 38
7. Implementering i organisationen 40
8. Opsummering 41

1. Forord

Ifølge databeskyttelsesforordningen gælder der en generel forpligtelse for dataansvarlige til at anmelde brud på persondatassikkerheden til Datatilsynet, medmindre at det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Samtidig har dataansvarlige en forpligtelse til at underrette de registrerede, hvis bruddet på persondatasikkerheden sandsynligvis vil indebære en høj risiko for deres rettigheder og frihedsrettigheder.

De dataansvarliges forpligtelse til at anmelde brud på persondatasikkerheden indebærer en række fordele, idet anmeldelse af brud bl.a. er et værktøj, der medvirker til, at beskyttelsen af de registreredes personoplysninger løbende forbedres, idet anmeldelserne gør Datatilsynet i stand til undersøge, hvordan bruddene behandles hos de dataansvarlige, herunder vurdere, om de dataansvarlige træffer passende foranstaltninger for at varetage de registreredes rettigheder. Datatilsynet kan på baggrund af en anmeldelse også vurdere, om de berørte personer skal underrettes om bruddet på persondatasikkerheden, så de berørte personer kan træffe forholdsregler for at beskytte sig selv mod bruddets potentielle konsekvenser.

Hvis den dataansvarlige ikke overholder sin forpligtelse til at anmelde brud på persondatasikkerheden til Datatilsynet og/eller underrette de registrerede, kan tilsynet gøre brug af sine korrigerende beføjelser. Datatilsynets korrigerende beføjelser kan f.eks. være at udtale kritik eller udstede påbud. Datatilsynet kan også – f.eks. med henblik på bødeindstilling – politianmelde en dataansvarlig for overtrædelse af reglerne, hvis omstændighederne i sagen taler for det. Politianmeldelse kan ske i kombination med eller i stedet for Datatilsynets korrigerende beføjelser.

Denne vejledning er målrettet de dataansvarlige private virksomheder, offentlige myndigheder, fysiske personer, institutioner og andre organer, som i tilfælde af et sikkerhedsbrud, der involverer personoplysninger, skal vurdere, om der i den forbindelse er pligt til at anmelde bruddet til Datatilsynet og pligt til at underrette de registrerede. Herudover indeholder vejledningen en gennemgang af de indholdsmæssige krav til en anmeldelse af et brud på persondatasikkerheden til Datatilsynet og underretning til de registrerede, ligesom der bliver redegjort for databeskyttelsesforordningens krav til tidspunktet for, hvornår der skal ske anmeldelse og underretning, herunder hvordan anmeldelsen skal indgives til Datatilsynet.

Er man som dataansvarlig i tvivl om, hvordan et brud på persondatasikkerheden skal håndteres – herunder om der skal ske anmeldelse af bruddet til Datatilsynet og/eller underretning af de registrerede – er man altid velkommen til at kontakte Datatilsynet (telefonisk) for at få råd og vejledning.

2. Hvornår er der sket et brud på persondatasikkerheden

2.1 Definition på et brud på persondatasikkerheden

For at kunne håndtere et brud på persondatasikkerheden, skal den dataansvarlige først være i stand til at genkende ét.

Brud på persondatasikkerheden

Et brud på persondatasikkerheden medfører ikke altid, at der skal ske anmeldelse til Datatilsynet og underretning af berørte registrerede. Det kan du læse mere om i del 3 og 4 af denne vejledning.

Man skal dog altid dokumentere brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet, bl.a. så Datatilsynet er i stand til at kontrollere, at man har håndteret bruddet korrekt. Det kan du læse mere om i del 5.

I databeskyttelsesforordningen defineres et brud på persondatasikkerheden på denne måde:

> *"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".*

Af definitionen følger, at to betingelser skal være opfyldt, før en hændelse kan kategoriseres som et brud på persondatasikkerheden.

For det første skal der altid være tale om et *brud på sikkerheden*. Det skal dermed være en hændelse, som bryder med eller afviger fra den dataansvarliges etablerede sikkerhedsforanstaltninger. Det kan f.eks. være et hackerangreb, hvor en ondsindet aktør lykkes med at forbigå sikkerhedsforanstaltninger f.eks. i form af en firewall, eller en medarbejder, der handler i strid med virksomhedens eller myndighedens retningslinjer og procedurer.

For det andet skal hændelsen føre til enten en *hændelig* eller *ulovlig* behandling af personoplysninger. Ved *hændelig* forstås, at noget sker utilsigtet eller ved en tilfældighed, f.eks. hvis en medarbejder utilsigtet fremsender personoplysninger til en forkert modtager. En *ulovlig* handling kan f.eks. være, hvis uvedkommende får adgang til personoplysninger gennem et hackerangreb eller tyveri af en computer, der indeholder personoplysninger.

Som udgangspunkt vil en *hændelig* handling, der fører til et brud på sikkerheden, imidlertid også være *ulovlig*, idet medarbejderen, der utilsigtet fremsender oplysninger til en forkert modtager, sandsynligvis ikke må videregive oplysningerne til den forkerte modtager.

Den hændelige og/eller ulovlige behandling skal herudover føre til en eller flere af følgende konsekvenser for personoplysninger:

- **Tilintetgørelse:** Hvis personoplysninger f.eks. slettes eller på anden måde destrueres, så de ikke længere findes eller ikke længere findes i en form, som virksomheden eller myndigheden kan behandle.
- **Tab:** Mistet adgang til kontrollen over eller adgangen til oplysninger, som virksomheden eller myndigheden før havde kontrol over eller adgang til. Tabet kan også være midlertidigt, f.eks. hvis en mistet adgang til et it-system, der indeholder personoplysninger, bliver genoprettet.
- **Ændring:** Når personoplysninger bliver ændret eller beskadiget, så de f.eks. er ukorrekte eller ufuldstændige.
- **Uautoriseret videregivelse og adgang:** Videregivelse af eller etablering af adgang til personoplysninger til/for personer, som ikke er autoriseret til at modtage eller få adgang til oplysningerne. Der vil være tale om uautoriseret adgang, selvom det kun har været muligt for en ikke-autoriseret person at tilgå personoplysningerne.
- **Ulovlig adgang til personoplysninger:** Hvis personoplysninger bliver tilgået på en måde, som ikke er tilladt, eksempelvis hvis en hacker skaffer sig adgang til personoplysninger, eller når en medarbejder, som handler i strid med lovgivning eller interne retningslinjer, tilgår personoplysninger, som personen ikke må tilgå, uanset om personen er autoriseret til tilgå oplysningerne eller ej.

En bevidst, tilsigtet handling fra den dataansvarlige vil derimod som det klare udgangspunkt ikke være et brud på persondatasikkerheden.

Det vil f.eks. ikke være et *brud* på den dataansvarliges etablerede sikkerhedsforanstaltninger, når den dataansvarlige bevidst videregiver oplysninger i den tro, at det er lovligt – hvis den dataansvarlige f.eks. er af den opfattelse, at videregivelsen har hjemmel i databeskyttelsesforordningen – men hvor det senere ved nærmere undersøgelse viser sig, at videregivelsen af oplysninger i det konkrete tilfælde ikke var lovlig.

I stedet er der tale om en tilsigtet handling, som kan være ulovlig, men som ikke er et brud på persondatasikkerheden.

Ved vurderingen af, om den dataansvarlige som overordnet ansvarlig har foretaget en tilsigtet, bevidst handling, bør det navnlig indgå, om personen eller personerne – f.eks. medarbejderen eller medarbejderne – der har udført handlingen på vegne af den dataansvarlige har handlet i overensstemmelse med den dataansvarliges etablerede arbejdsgange, retningslinjer, procedurer og processer i forbindelse med udførelsen af opgaver, som personen eller personerne er blevet pålagt af den dataansvarlige.

Der vil kun være tale om et brud på persondatassikkerheden i databeskyttelsesretlig forstand, hvis bruddet involverer personoplysninger. Derimod vil en informationssikkerhedshændelse ikke nødvendigvis udgøre et brud på persondatasikkerheden. ISO 27000-standarden definerer en informationssikkerhedshændelse som:

"En identificeret forekomst af en system-, tjeneste- eller netværkstilstand, der indikerer et muligt brud på informationssikkerhedspolitikken eller svigt af kontroller, eller en tidligere ukendt situation, der kan være relevant for sikkerheden…"

Derfor vil f.eks. flere forgæves forsøg på log-in af uvedkommende være en informationssikkerhedshændelse, men dette vil ikke være et brud på persondatasikkerheden, fordi hændelsen ikke har ført til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger.

2.2 Informationssikkerhedsrisici og brud på persondatasikkerheden

Brud på persondatasikkerheden kan kategoriseres efter tre informationssikkerhedsrisici[1]:

- *"Brud på fortrolighed"* – uautoriseret eller hændelig videregivelse af eller adgang til personoplysninger.
- *"Brud på integritet"* – uautoriseret eller hændelig ændring af personoplysninger.
- *"Brud på tilgængelighed"* – uautoriseret eller hændeligt tab af adgang til eller tilintetgørelse af personoplysninger.

Et brud på persondatasikkerheden kan omfatte én eller flere af ovenstående informationssikkerhedsrisici. Det kan være forholdsvis enkelt at fastslå, om der foreligger et brud på fortroligheden eller integriteten, hvorimod det kan være mere kompliceret at fastslå, om der foreligger et brud på tilgængeligheden. Dette skyldes, at perioden, hvor personoplysninger er utilgængelige, karakteren af oplysningerne og konsekvensen forbundet med utilgængeligheden af oplysningerne har betydning for, om der er tale om et brud på persondatassikkerheden, idet et kortvarigt, midlertidigt tab af tilgængelighed til oplysninger, der ikke medfører en konsekvens for de registrerede, ikke nødvendigvis vil være et brud på persondatasikkerheden.

2.3 Eksempler på brud

Følgende er eksempler på informationssikkerhedshændelser, der – afhængig af de konkrete omstændigheder – kan være brud på persondatasikkerheden. Eksemplerne er i nogle tilfælde opdelt i flere scenarier, hvor de konkrete omstændigheder enten medfører, at der er tale om et brud på persondatasikkerheden, eller at der ikke er tale om et brud på persondatasikkerheden. Flere af eksemplerne indeholder også et scenarie, hvor det er op til en konkret vurdering, om der er tale om et brud på persondatasikkerheden.

Der er taget udgangspunkt i de brud, som er beskrevet i Datatilsynets vejledning om 10 typiske brud på persondatasikkerheden, og de scenarier, der beskrives i EDPB's retningslinjer om anmeldelse af brud på persondatasikkerheden[2].

Hvor der er tale om brud på persondatasikkerheden, fremhæves det, hvilken type brud der er tale om, så det kan sammenholdes med definitionen på brud. Endvidere fremhæves typen af informationssikkerhedsrisici.

1 Artikel 29-gruppens udtalelse om "Opinion 03/2014 on Personal Data Breach Notification", WP 213. Personal Data Breach Notification – typical use cases requiring notification to individuals (europa.eu)

2 Retningslinjer 01/2021 om eksempler på anmeldelse af brud på persondatasikkerheden. Vedtaget den 14. december 2021. Version 2.0

Eksempel 1: Flytbart medie bliver stjålet

En PC, USB-nøgle eller andet flytbart medie med personoplysninger bliver stjålet. Her er nogle af de tænkelige scenarier:

a) **Personoplysningerne på mediet er ikke krypteret.**
Hvis personoplysningerne på mediet ikke er krypteret, vil det være et brud på sikkerheden, der medfører en **ulovlig, uautoriseret** adgang til personoplysninger, idet tyven – som ikke er autoriseret til at tilgå personoplysningerne – på grund af den manglende kryptering vil have adgang til oplysningerne, uanset om adgangen rent faktisk er udnyttet. Hændelsen er et informationssikkerhedsbrud på oplysningernes **fortrolighed**.

b) **Personoplysningerne eller hele mediet er beskyttet af en stærk kryptering, der ikke kan omgås.**
Det er ikke et brud, fordi man kan lægge til grund, at tyven ikke har mulighed for at dekryptere de data, der ligger på det stjålne medie, hvorfor der ikke har været uautoriseret adgang til personoplysningerne.

c) **Personoplysningerne eller hele mediet er krypteret, men krypteringen er svag, eller der er tvivl om, hvorvidt den kryptografiske nøgle var ordentligt beskyttet, eller om det er muligt at prøve sig frem til adgangskoden, som kan dekryptere data på mediet.**
I denne situation skal det overvejes, om krypteringen er så svag, at det vil være muligt for tyven at bryde krypteringen og få adgang til personoplysningerne. Det kan bl.a. afhænge af krypteringsnøglens længde, og hvor lang tid det vil tage for den ondsindede person at bryde krypteringen.[3]

Eksempel 2: Oplysningerne mistes

En pc indeholdende de *eneste* eksemplarer af krypterede personoplysninger bliver stjålet. Krypteringen gør oplysningerne utilgængelige for uvedkommende.

Det er et brud på sikkerheden, der medfører et **tab af personoplysninger** for den dataansvarlige, fordi den dataansvarlige ikke længere er i besiddelse af oplysningerne. Hændelsen er et informationssikkerhedsbrud på oplysningernes **tilgængelighed.**

Hvis personoplysningerne bliver tilgængelige for den dataansvarlige igen, f.eks. ved at pc'en genfindes uskadt, vil der være tale om et **midlertidigt tab af personoplysninger** for den dataansvarlige, som sandsynligvis er et brud – det afhænger af, hvor lang tid det midlertidige tab varede, og om det havde en negativ indvirkning på de personer, hvis oplysninger var utilgængelige (de registrerede).

3 Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer 1. udgave (2020) s. 647ff.

Eksempel 3: Hacker får adgang til oplysninger

En hacker bryder ind i et it-system og får adgang til personoplysninger. Det er ikke muligt at fastslå, om hackeren også har hentet (downloadet eller ekstraheret) eller ændret personoplysninger. Her er nogle af de tænkelige scenarier:

a) **Hackeren har kun adgang til oplysningerne.**
Hændelsen er et brud på sikkerheden, der medfører **ulovlig, uautoriseret adgang til personoplysninger** i it-systemet, fordi hackeren som minimum har adgang til oplysningerne uden at være autoriseret til det. Det er et informationssikkerhedsbrud på oplysningernes **fortrolighed**.

b) **Hackeren ændrer eller sletter oplysninger.**
Hvis hackeren ændrer eller på anden måde redigerer i personoplysninger, vil det også være **ulovlig ændring af personoplysninger**. Hvis hackeren også sletter oplysningerne eller ændrer dem, så den dataansvarlige ikke længere kan tilgå de oprindelige oplysninger – f.eks. gennem backup – er det et **tab af personoplysninger**. Hændelsen kan dermed også udgøre et informationssikkerhedsbrud på oplysningernes **integritet** og/eller **tilgængelighed**.

Eksempel 4: Hacker prøver at få adgang

En hacker forsøger at få adgang til et system, f.eks. ved at prøve at logge ind med forskellige adgangskoder eller ved phishing. Her er nogle af de tænkelige scenarier:

a) **Hændelsen resulterer ikke i en etablering af adgang til personoplysninger.**
Hvis hændelsen ikke resulterer i etablering af adgang til oplysninger for uvedkommende, vil der være tale om en "informationssikkerhedshændelse", som ikke er et brud på persondatasikkerheden, idet hændelsen ikke har ført til uautoriseret adgang til personoplysninger.

b) **Hændelsen resulterer i etablering af adgang til personoplysninger.**
Hvis hændelsen resulterer i etablering af adgang til oplysninger for uvedkommende, vil der være tale om et brud på persondatasikkerheden, der medfører **uautoriseret, ulovlig adgang til personoplysninger,** som endvidere kan føre til **ændring og tab af personoplysninger**. Det afhænger af hvilke rettigheder, der opnås gennem log-in. Det kan dermed udgøre et informationssikkerheds-brud på oplysningernes, **fortrolighed, integritet og/eller tilgængelighed**.

Eksempel 5: Sårbarhed i firewall

Der eksisterer en sårbarhed på en firewall mod internettet, der kan udnyttes til at få adgang til personoplysninger. Her er nogle af de tænkelige scenarier:

a) **Sårbarheden er kendt og meget nem at udnytte.**
Det er et brud på sikkerheden, der indebærer en **ulovlig, uautoriseret adgang til personoplysninger**, fordi uvedkommende nemt kan opnå adgang til personoplysningerne. Hændelsen er et informations-sikkerhedsbrud på oplysningernes **fortrolighed**.

Det er et brud, uanset om sårbarheden har været udnyttet eller ej.

b) **Sårbarheden er ikke kendt og kan kun udnyttes af (dygtige) hackere med særlig kendskab/særlige egenskaber. Sårbarheden er ikke blevet udnyttet.**
Det er ikke et brud, fordi det ikke er nemt at opnå adgang, idet en udnyttelse af sårbarheden kræver særlige kompetencer, som kun (dygtige) hackere må forventes at have.

c) **Sårbarheden er kendt, men personoplysninger er gemt bag flere lag af sikkerhed, hvilket medfører, at personoplysninger – trods udnyttelse af sårbarheden i firewallen – ikke kan tilgås.**
Det er ikke et brud, fordi der ikke har været uautoriseret adgang til personoplysninger, idet firewallen kun udgør en del af den samlede beskyttelse af personoplysninger, og de andre dele af denne beskyttelse ikke har været kompromitteret.

Eksempel 6: Ramt af ransomware

En dataansvarlig bliver udsat for et ransomwareangreb, hvor personoplysninger i it-systemer krypteres og "holdes som gidsel". Oplysningerne bliver utilgængelige for den dataansvarlige på en måde, så den dataansvarlige ikke kan behandle oplysningerne til de tilsigtede formål – f.eks. sagsbehandling, kundeadministration eller behandling af en borger på et sygehus. Her er nogle af de tænkelige scenarier:

a) **Krypteringen sker ved ondsindet software, som er sendt ind i et it-system, hvor det har ageret uden menneskelig indgriben. Dette kan dokumenteres (f.eks. via logs). Uvedkommende personer har derfor ikke haft adgang til oplysninger, og oplysninger er derudover ikke udtrukket (downloadet eller ekstraheret).**
Det er et brud på sikkerheden, der som minimum medfører **ændring af** og et midlertidigt **tab af personoplysninger**, indtil f.eks. en backup er anvendt til at genetablere oplysningerne. Krypteringen er en ændring af data, og personoplysningerne er (midlertidigt) tabt, fordi de ikke er tilgængelige for den dataansvarlige. Det er et informationssikkerhedsbrud på oplysningernes **integritet** og **tilgængelighed**.

b) **Før krypteringen blev udført, er personoplysninger (og andre data) blevet udtrukket og gjort tilgængelige for uvedkommende.**
Det er et brud på sikkerheden, der som minimum medfører **ændring af** og et midlertidigt **tab af personoplysninger**, men derudover har der også været **ulovlig, uautoriseret adgang til personoplysninger**, fordi data er udtrukket (og muligvis tilgået) af uvedkommende. Det er et informationssikkerhedsbrud på oplysningernes **fortrolighed, integritet** og **tilgængelighed**.

c) **Ransomwareangrebet medfører, at oplysninger bliver ødelagt. Samtidig kan personoplysningerne ikke genskabes ved hjælp af en backup.**
Det er sket et brud på sikkerheden, der **medfører ulovlig tilintetgørelse af personoplysninger**. Det er et informationssikkerhedsbrud på oplysningernes **tilgængelighed**.

Eksempel 7: Papirer med oplysninger bliver stjålet

Der stjæles et papirregister med personoplysninger (f.eks. en logbog over fremmøde i misbrugscenter). Der er ingen kopi af dette register.

Det er et brud på sikkerheden, der medfører **ulovlig, uautoriseret adgang til personoplysninger** idet tyven har adgang til oplysningerne. Da oplysningerne kun fremgik af dette papirregister, er der også sket et **tab af personoplysninger**. Det er et informationssikkerhedsbrud på oplysningernes **fortrolighed og tilgængelighed**.

Eksempel 8: Vandskade på server

En vandskade ødelægger servere med personoplysninger. Der er ikke en brugbar backup af personoplysningerne.

Det er et brud på sikkerheden, der medfører **hændelig tilintetgørelse**, fordi personoplysninger ikke kan genskabes. Det er et informationssikkerhedsbrud på oplysningernes **tilgængelighed**.

Eksempel 9: Nedbrud i system

Der er nedbrud i et it-system, men der er en brugbar backup af personoplysninger og it-systemernes software.

Det er et brud på sikkerheden, der medfører midlertidigt **tab af personoplysninger** idet det antages, at backup kan anvendes til at genetablere den dataansvarliges adgang til oplysningerne. Det er et informationssikkerhedsbrud på oplysningernes **tilgængelighed**.

Eksempel 10: Planlagt nedetid

Den dataansvarlige får udført planlagt vedligeholdelse af et it-system, hvorfor personoplysningerne, der bliver behandlet i systemet, er utilgængelige i den planlagte periode.

Det er ikke et brud på persondatasikkerheden, fordi det er en bevidst handling udført af den dataansvarlige at tage systemet ud af brug i en periode for at udføre vedligeholdelse.

Eksempel 11: Medarbejder videregiver oplysninger ulovligt

En medarbejder anvender autoriseret adgang til at tilgå personoplysninger og sender disse til en uvedkommende tredjepart, uden at der er et arbejdsbetinget behov for nogen af delene.

Det er et brud på sikkerheden, der medfører **ulovlig adgang til personoplysninger**. Selvom medarbejderen har autoriseret adgang til at tilgå personoplysningerne, er der tale om, at adgangen anvendes ulovligt, idet medarbejderen ikke har et arbejdsbetinget behov for at tilgå dem.

Da medarbejderen sender personoplysninger til en uvedkommende tredjepart, er der også sket en **ulovlig videregivelse af personoplysninger**. Se også illustrationen i eksempel 13.

Begge hændelser er et informationssikkerhedsbrud på oplysningernes **fortrolighed**.

Eksempel 12: Oplysninger til forkert modtager

Der sendes et brev til en korrekt modtager, hvoraf der fejlagtigt fremgår oplysninger om en uvedkommende tredjemand. Eller der sendes et brev til en forkert modtager, hvoraf der fremgår personoplysninger, som den forkerte modtager ikke skulle have.

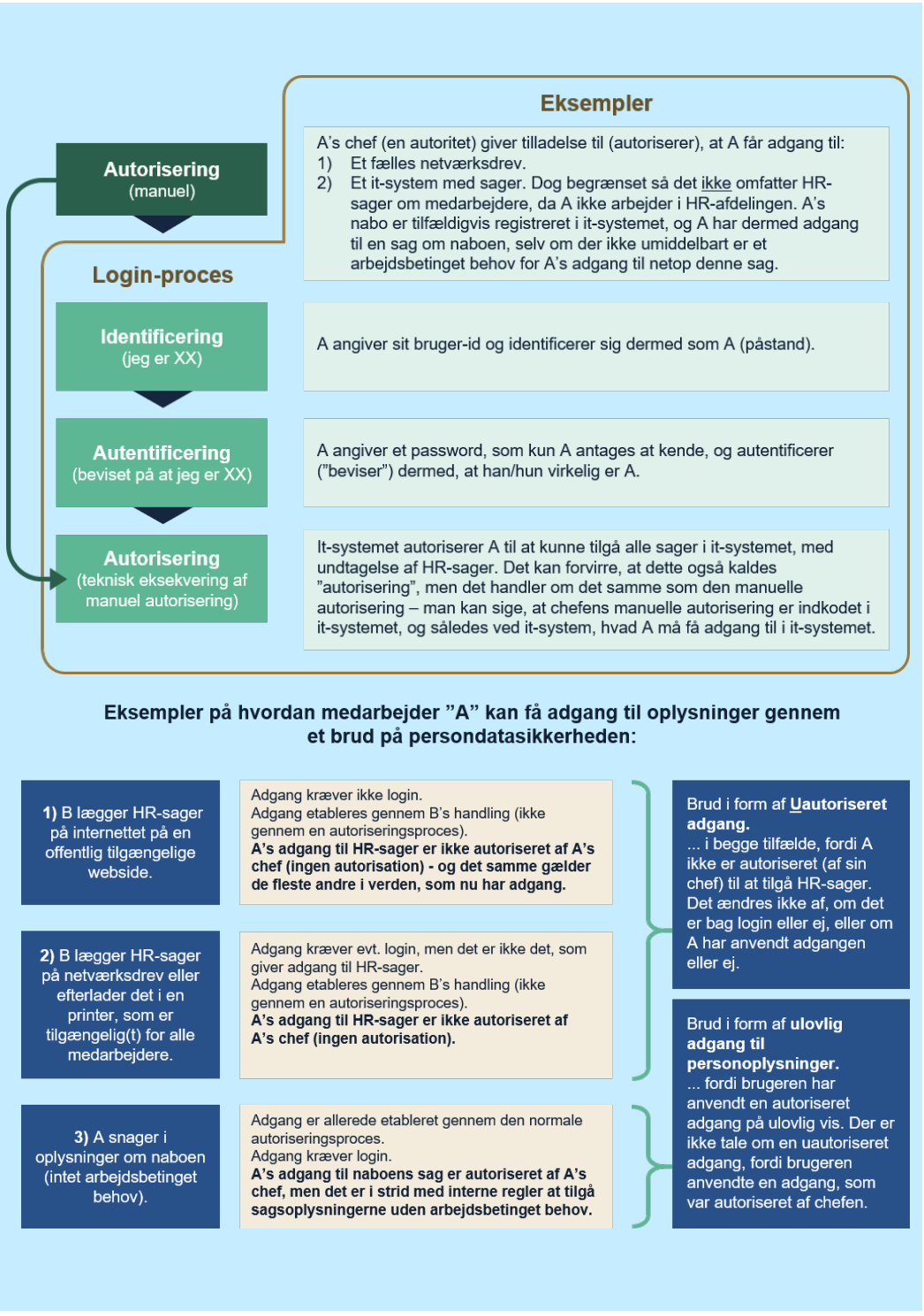
Det er i begge tilfælde et brud på sikkerheden, der medfører en **hændelig, ulovlig videregivelse af personoplysninger**. Idet modtageren i begge situationer ikke er autoriseret til at få adgang til personoplysningerne, har det også medført **hændelig, uautoriseret adgang til oplysningerne**. Det er et informationssikkerhedsbrud på oplysningernes **fortrolighed**.

Eksempel 13: Uautoriseret adgang

Utilstrækkelig adgangsbegrænsning til personoplysninger i f.eks. en mappe, et fildrev eller cloudløsning medfører, at personer – f.eks. medarbejdere i en virksomhed eller myndighed – der ikke er autoriseret til at tilgå oplysningerne, alligevel har mulighed for at tilgå dem. Her er nogle af de tænkelige scenarier:

a) **Log eller andre tilsvarende sikkerhedsforanstaltninger viser, at oplysninger ikke blevet tilgået af uautoriseret personer.**
   Det er et brud på sikkerheden, der medfører **uautoriseret adgang til personoplysninger**, fordi medarbejdere har en adgang, som de ikke er autoriseret til. Så snart det er muligt for en ikke-autoriseret person at tilgå personoplysninger, er der etableret "uautoriseret adgang". Det er uden betydning i denne sammenhæng, om der er tegn på anvendelse af adgangen eller ej. Det er et informationssikkerhedsbrud på oplysningernes **fortrolighed**.

b) **Logs eller andre tilsvarende sikkerhedsforanstaltninger viser, at oplysninger er blevet tilgået af uautoriseret personer og slettet eller ændret.**
   Der er et brud på sikkerheden, der medfører **hændelig eller ulovlig ændring af personoplysninger**, fordi loggen viser, at en uautoriseret person har benyttet sig af adgangen til at ændre i eller slette data. Dermed er integriteten også berørt.


Eksempler
Autorisering
(manuel)
A's chef (en autoritet) giver tilladelse til (autoriserer), at A får adgang til:
1) Et fælles netværksdrev.
2) Et it-system med sager. Dog begrænset så det ikke omfatter HR-sager om medarbejdere, da A ikke arbejder i HR-afdelingen. A's nabo er tilfældigvis registreret i it-systemet, og A har dermed adgang til en sag om naboen, selv om der ikke umiddelbart er et arbejdsbetinget behov for A's adgang til netop denne sag.
Login-proces
Identificering
(jeg er XX)
A angiver sit bruger-id og identificerer sig dermed som A (påstand).
Autentificering
(beviset på at jeg er XX)
A angiver et password, som kun A antages at kende, og autentificerer ("beviser") dermed, at han/hun virkelig er A.
Autorisering
(teknisk eksekvering af manuel autorisering)
It-systemet autoriserer A til at kunne tilgå alle sager i it-systemet, med undtagelse af HR-sager. Det kan forvirre, at dette også kaldes "autorisering", men det handler om det samme som den manuelle autorisering – man kan sige, at chefens manuelle autorisering er indkodet i it-systemet, og således ved it-system, hvad A må få adgang til i it-systemet.
Eksempler på hvordan medarbejder "A" kan få adgang til oplysninger gennem et brud på persondatasikkerheden:
1) B lægger HR-sager på internettet på en offentlig tilgængelige webside.
Adgang kræver ikke login.
Adgang etableres gennem B's handling (ikke gennem en autoriseringsproces).
A's adgang til HR-sager er ikke autoriseret af A's chef (ingen autorisation) - og det samme gælder de fleste andre i verden, som nu har adgang.
2) B lægger HR-sager på netværksdrev eller efterlader det i en printer, som er tilgængelig(t) for alle medarbejdere.
Adgang kræver evt. login, men det er ikke det, som giver adgang til HR-sager.
Adgang etableres gennem B's handling (ikke gennem en autoriseringsproces).
A's adgang til HR-sager er ikke autoriseret af A's chef (ingen autorisation).
3) A snager i oplysninger om naboen (intet arbejdsbetinget behov).
Adgang er allerede etableret gennem den normale autoriseringsproces.
Adgang kræver login.
A's adgang til naboens sag er autoriseret af A's chef, men det er i strid med interne regler at tilgå sagsoplysningerne uden arbejdsbetinget behov.
Brud i form af Uautoriseret adgang.
... i begge tilfælde, fordi A ikke er autoriseret (af sin chef) til at tilgå HR-sager. Det ændres ikke af, om det er bag login eller ej, eller om A har anvendt adgangen eller ej.
Brud i form af ulovlig adgang til personoplysninger.
... fordi brugeren har anvendt en autoriseret adgang på ulovlig vis. Der er ikke tale om en uautoriseret adgang, fordi brugeren anvendte en adgang, som var autoriseret af chefen.

Eksempel 14: Utilsigtet offentliggørelse

Ved en fejl offentliggøres personoplysninger på internettet.

Det er et brud på sikkerheden, der medfører **uautoriseret, ulovlig adgang til personoplysninger**, idet personoplysningerne utilsigtet er blevet gjort tilgængelige for brugere af internettet, der ikke er autoriserede til at tilgå oplysningerne. Se illustration i eksempel 13.

Eksempel 15: Transmission uden kryptering

Personoplysninger er f.eks. i en mail transmitteret over internettet uden anvendelse af kryptering.

Det er et brud på sikkerheden, der medfører **uautoriseret adgang til personoplysninger**, fordi usikker transmission af oplysninger over et netværk som internettet medfører, at der er adgang til personoplysningerne i ikke-krypteret form under transmissionen. Det er et informationssikkerhedsbrud på oplysningernes **fortrolighed**.

Eksempel 16: Fejl i systemintegration

En fejl fører til, at der ikke udveksles (korrekte) oplysninger mellem to systemer, hvilket medfører, at oplysningerne i et eller begge systemer ændres og er ukorrekte – f.eks. overføres oplysninger om adressebeskyttelse ikke korrekt fra et system til et andet, hvilket resulterer i, at en person mister sin adressebeskyttelse. Her er nogle af de tænkelige scenarier:

a) **Oplysningerne er ukorrekte i et eller begge systemer, men bliver ikke tilgængelige for uvedkommende.**
Det er et brud på sikkerheden, der medfører en **hændelig ændring af personoplysninger**, fordi oplysningerne ændres – f.eks. mister en person sin adressebeskyttelse. Det er et informationssikkerhedsbrud på oplysningernes **integritet**.

b) **De ukorrekte oplysninger medfører, at oplysninger bliver tilgængelige for uvedkommende**.
Det er et brud på sikkerheden, der medfører **ulovlig videregivelse af personoplysninger** – f.eks. bliver en beskyttet adresse offentliggjort eller videregivet til uvedkommende. Hændelsen er et informationssikkerhedsbrud på **fortroligheden**.

Eksempel 17: Fejl ved alarmknap

En borger har fået en alarmopkaldsknap af kommunen. Alarmopkaldsknappen er en del af en it-løsning – en service – som kommunen udbyder, og kommunen er i situationen ansvarlig for behandlingen af personoplysninger i løsningen. Der er en kobling mellem knappen og borgerens adresse, så kommunen ved, hvor borgeren befinder sig, hvis borgeren trykker på knappen. Grundet en fejl virker knappen ikke, da borgeren trykker på den, og ingen bliver opmærksomme på borgerens nødsituation.

Det er et brud på sikkerheden, der medfører et **hændeligt tab af personoplysninger**, idet informationen om borgerens nødsituation ikke når frem til kommunen. Det er et informationssikkerhedsbrud på oplysningernes **tilgængelighed**, fordi informationen om at en borger er i problemer, ikke tilgår den, som skal hjælpe borgeren.

3. Anmeldelse til Datatilsynet

3.1 Hvordan foretages anmeldelse til Datatilsynet?

Der er etableret en fælles indberetningsløsning, hvor virksomheder og myndigheder kan anmeldelse sikkerhedshændelser – herunder brud på persondatasikkerheden – på hjemmesiden www.virk.dk, som i øvrigt allerede fungerer som den digitale indgang, hvor virksomheder og myndigheder kan indberette forskellige forhold til det offentlige.

Indberetningsløsningen gør det nemt og enkelt for virksomheder og myndigheder at indberette (sikkerheds)hændelser til flere myndigheder samtidig, hvis hændelsen er omfattet af krav om anmeldelse til flere forskellige myndigheder. Løsningen forsøger samtidig at sikre, at der afgives de nødvendige oplysninger, uden at brugeren af løsningen (anmelderen) skal kende alle (lov)kravene til anmeldelse.

Der vil altid være et opdateret link til den nuværende indberetningsløsning på Datatilsynets hjemmeside.

3.2 Hvilke brud på persondatasikkerheden kræver anmeldelse?

Som udgangspunkt skal brud på persondatasikkerheden anmeldes til Datatilsynet, med mindre, at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder

> En risiko for fysiske personers rettigheder og frihedsrettigheder betyder, at der kan være en risiko for, at et brud på persondatasikkerheden f.eks. kan have konsekvenser for registrerede i form af diskrimination, identitetstyveri eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden væsentlig økonomisk eller social ulempe for den registrerede.

Hvis en dataansvarlig undlader at anmelde et brud på persondatasikkerheden til Datatilsynet, kan det f.eks. resultere i, at Datatilsynet udtaler kritik eller udsteder et påbud til den dataansvarlige om at foretage anmeldelse af bruddet. Afhængig af omstændighederne i hver enkelt sag, kan Datatilsynet imidlertid også sanktionere den manglende efterlevelse af reglerne med bøde – enten i kombination med eller i stedet for en af Datatilsynets andre korrigerende beføjelser.

Hensynet bag, at manglende efterlevelse af reglerne om at anmelde et brud på persondatasikkerheden kan føre til sanktioner, skyldes primært, at Datatilsynet ikke er i stand til at vurdere, om en dataansvarlig har håndteret et brud korrekt, hvis tilsynet ikke er bekendt med at bruddet har fundet sted. Datatilsynet vil derfor f.eks. ikke kunne sikre, at den dataansvarlige har standset bruddet, ryddet op efter bruddet og truffet passende foranstaltninger for, at bruddet ikke gentager sig. Herudover vil Datatilsynet ikke være i stand til at vurdere, om der er sket (korrekt) underretning af de berørte registrerede.

Den dataansvarlige skal straks efter at være blevet bekendt med bruddet på persondatasikkerheden vurdere sandsynligheden for, at bruddet indebærer en risiko for de berørte fysiske personers rettigheder.

Begrebet ”risiko” indebærer en *sandsynlighed* for et negativt udfald og en *konsekvens/alvor* ved det negative udfald. Vurderingen skal derfor angå de mulige negative konsekvenser ved bruddet for de personer, hvis oplysninger er berørt, og sandsynligheden for, at konsekvenserne indtræffer.

Følgende forhold bør altid indgå i den konkrete vurdering af risikoen for de registreredes rettigheder og frihedsrettigheder som følge af et brud på persondatasikkerheden, idet forholdene i kombination har betydning for *sandsynlighed* og *konsekvens*, der tilsammen udgør risikoen:

- Typen af sikkerhedsbrud
- Oplysningernes type og mængde;
- Muligheden for, at registrerede kan identificeres;
- Hvem, der eventuelt uretmæssigt har fået adgang til oplysningerne;
- Bruddets varighed;
- Særligt sårbare berørte;
- Antallet af fysiske personer, hvis personoplysninger er omfattet af bruddet.

Læs mere om eksempler på, hvornår der skal foretages anmeldelse af brud på persondatasikkerheden til Datatilsynet under afsnit 3.8 nedenfor.

3.2.1 Typen af brud

Se afsnit 2.2 for eksempler på typer af brud.

Hvilke konsekvenser, som et brud på persondatasikkerheden kan få for de berørte personer, afhænger bl.a. af, hvilken type af brud, der er tale om. Et brud, der indebærer, at personoplysninger ikke længere er tilgængelige, kan således få nogle helt andre konsekvenser for den registrerede, end hvis der f.eks. er tale om et brud, der resulterer i offentliggørelse af personoplysninger.

3.2.2 Kategorier og mængden af oplysninger

Som udgangspunkt vil *kategorien* af oplysninger have indflydelse på risikovurderingen.

Eksempelvis må en utilsigtet videregivelse eller offentliggørelse af oplysninger om, at en person har begået strafbare forhold, har opbygget en stor gæld eller lider af en bestemt sygdom formodes at kunne få mere vidtrækkende konsekvenser for den pågældende, end hvis f.eks. den pågældendes e-mailadresse eller CV bliver utilsigtet videregivet eller offentliggjort.

Det betyder imidlertid ikke, at utilsigtet adgang til f.eks. en e-mailadresse eller et CV ikke (også) kan få konsekvenser for en registreret. Et CV kan indeholde fortrolige oplysninger som et personnummer, og afhængig af bruddets karakter, kan utilsigtet adgang til et CV f.eks. afsløre, at et en medarbejder søger væk fra sin nuværende arbejdsgiver.

Det kan muligvis også få alvorlige konsekvenser for en registreret, hvis dennes e-mailadresse kommer til hackeres kendskab ved et hackerangreb hos en dataansvarlig, fordi hackerne nu også ved, at den registrerede har kommunikeret med den dataansvarlige. Hackerne kan herefter anvende oplysningerne til målrettede phishing-angreb, hvor den registrerede lokkes til at udlevere personoplysninger, eller hvor den registrerede lokkes til hjemmesider, der spreder ondsindet software.

En risikovurdering skal derfor ikke blot tage udgangspunkt i, hvilke kategorier af oplysninger, der er blevet kompromitteret ved et brud, men skal også tage udgangspunkt i, hvem der f.eks. har fået adgang til oplysningerne, og hvordan oplysningerne kan misbruges.

Man skal i den forbindelse tage alle omstændigheder omkring sikkerhedsbruddet i betragtning, herunder de særlige hensyn, der kan gøre sig gældende for de personer, hvis oplysninger f.eks. er blevet eksponeret. Offentliggørelse af adresseoplysninger vil f.eks. normalt ikke forventes at kunne få alvorlige konsekvenser, hvorimod det kan forholde sig anderledes, hvis adressen afslører, at den pågældende er bosiddende på et bosted for personer i misbrugsbehandling, eller hvis vedkommende har adressebeskyttelse. Det samme kan gøre sig gældende for kendte personer eller personer under vidnebeskyttelse.

Mængden af personoplysninger, der er berørt af et brud, har ligeledes betydning for vurderingen. Det gælder både mængden af oplysninger om enkelte registrerede og den totale mængde af berørte oplysninger.

Typisk vil det være sådan, at jo flere oplysninger om en registreret, der er berørt af et brud, jo højere vil risikoen for misbrug af oplysningerne for den registrerede alt andet lige være, men antallet af f.eks. forkerte modtagere vil også have en betydning for vurderingen, selvom mængden af personoplysninger er lille.

Hvis en enkelt e-mailadresse er sendt til én forkert modtager, indebærer det nødvendigvis ikke, at det sandsynligvis medfører en høj risiko, men hvis mange e-mailadresser utilsigtet er blevet delt med mange modtagere, vil der være sket en spredning af personoplysningerne, der betyder, at der f.eks. vil være større sandsynlighed for, at én af modtagerne kan blive offer for ondsindede aktører, der udtrækker samtlige e-mailadresser med henblik på at anvende dem til et ondsindet formål.

Antallet af berørte personer eller berørte personoplysninger bør derfor indgå i risikovurderingen, men er ikke alene afgørende for udfaldet af en risikovurdering.

3.2.3 Muligheden for at identificere personer

Ved brud, der angår uautoriseret adgang til data, påvirkes risikovurderingen af, hvor svært det er at identificere personer ud fra de oplysninger, som der var uautoriseret adgang til.

Det mindsker i den forbindelse risikoen, hvis oplysningerne var beskyttet ved f.eks. kryptering eller pseudonymisering[4].

3.2.4 Mulige konsekvenser for de berørte personer

I databeskyttelsesforordningen er nævnt en række eksempler på, hvilke konsekvenser et brud på persondatasikkerheden kan have for fysiske personer. Der kan f.eks. være tale om:

- Fysisk skade
- Materiel skade
- Immateriel skade
- Forskelsbehandling
- Identitetstyveri
- Identitetssvig
- Økonomiske konsekvenser, herunder finansielle tab
- Skade på omdømme
- Sociale konsekvenser
- Indflydelse på privatliv
- Skade på menneskelig værdighed
- Skade på legitime interesser
- Begrænsning/krænkelse af fundamentale rettigheder og frihedsrettigheder
- Manglende udøvelse af kontrol med egne personoplysninger.

I et tilfælde, hvor personoplysninger – herunder fulde navn, adresse og helbredsoplysninger – i en livsforsikring er blevet tilgået af uvedkommende, kunne de sandsynlige konsekvenser til illustration være:

- Offentliggørelse af oplysninger om den registrerede på internettet, som f.eks. kan påvirke den registreredes mulighed for at finde et arbejde eller lignende (på baggrund af oplysninger om helbredsproblemer, graviditet mv.)
- Følelsesmæssig påvirkning af den registrerede, hvis den registrerede skjuler sin diagnose
- Identitetstyveri
- Oplysningerne kan blive udnyttet til phishing.

Konsekvenserne kan være umiddelbare, men kan også ligge langt ude i fremtiden. Man skal altså overveje, hvad bruddet kan forårsage på kort og lang sigt, uanset, om bruddet er

[4] Ved "pseudonymisering" forstås ifølge persondataforordningens artikel 4 nr. 5,: 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.

standset. Det kan også være relevant at vurdere, om konsekvenserne allerede kan have manifesteret sig tidligere, f.eks. hvis bruddet har stået på i lang tid.

3.2.5 Hvem, der eventuelt har fået uretmæssig adgang til personoplysningerne

Hvis den dataansvarlige ved, at de involverede personoplysninger er endt i hænderne på kriminelle personer – f.eks. hackere eller offentliggørelse på "dark web" – skal det forventes, at de har onde hensigter med deres kendskab til oplysningerne, og dette skal indgå i risikovurderingen.

Hvis den dataansvarlige ved, hvilke personer/organisationer, der har fået uautoriseret adgang til personoplysninger – f.eks. fordi oplysninger er sendt til en forkert modtager – kan modtageres troværdighed medregnes i risikovurderingen.

Det kan herunder vurderes, om den dataansvarlige har stor tillid til den uautoriserede part, og/eller om den uatoriserede part almindeligvis behandler typen af oplysninger, som de utilsigtet fik adgang til.

Det kan også indgå i vurderingen, om parten, der uatoriseret har fået adgang, f.eks. er underlagt en lovbestemt tavshedspligt eller lignende, men man skal altid have for øje, at en tavshedspligt i sig selv ikke betyder, at der ikke er en risiko for, at den uatoriserede part kan misbruge oplysningerne.

Hvis man som dataansvarlig ikke har kendskab til, om personoplysninger er kommet til uvedkommendes kendskab, bør dette nødvendigvis ikke være udslagsgivende for, om risikoen ved bruddet er lav, idet manglende viden om omstændighederne ved et brud som udgangspunkt øger den mulige risiko, som bruddet indebærer, og man bør derfor tage udgangspunkt i det værst tænkelige scenarie. Foranstaltninger som netværksovervågning, logning og lignende kan forhindre at denne situation opstår.

3.2.6 Bruddets varighed

Den *tidsmæssige udstrækning af et brud* har også betydning for vurderingen, da det alt andet lige må forudsættes, at risikoen for de registrerede er højere, hvis oplysninger på grund af et brud på persondatasikkerheden har været fejlbehæftede, utilgængelige eller tilgængelige for uvedkommende i en længere periode.

Risikoen kan dog påvirkes af, om man kan dokumentere, hvad der er sket i den periode, hvor bruddet har stået på, herunder om oplysningerne aldrig har været tilgået eller udnyttet/misbrugt.

3.2.7 Særligt sårbare registrerede

Et brud kan vurderes at have større skadevirkninger, hvis bruddet har medført kompromittering af oplysninger om særligt sårbare eller udsatte personer.

Det kan f.eks. være børn, syge personer, socialt udsatte personer eller personer, der af andre årsager kan opleve alvorligere konsekvenser ved bruddet.

I vurderingen skal også indgå, at nogle grupper af særligt sårbare eller udsatte personer kan have svært ved at forstå og håndtere konsekvenserne ved et brud, herunder tage fornødne forholdsregler for at beskytte sine rettigheder eller frihedsrettigheder.

3.2.8 Antallet af berørte personer

Som udgangspunkt vil den generelle risiko ved et brud på persondatasikkerheden stige i takt med antallet af personer, der er berørt af bruddet, men man skal som dataansvarlig huske at vurdere risikoen for hver enkelt registreret. Et brud vil derfor som udgangspunkt skulle anmeldes til Datatilsynet, selvom bruddet kun indebærer risiko for én ud af mange berørte.

Vurderingen af, om man skal anmelde bruddet til Datatilsynet, kan derfor ikke tage udgangspunkt i en bred risikovurdering, der er baseret på, hvordan risikoen for de fleste berørte er ved bruddet, hvis der er individer, som bliver udsat for en særlig risiko.

Relevante bestemmelser mv.

- Forordningens artikel 33, stk. 1
- Præambelbetragtning nr. 75, 76, 85, 86 og 87

3.3 Tidspunktet for anmeldelse

Med mindre, at det er usandsynligt, at et brud på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal den dataansvarlige *uden unødig forsinkelse og om muligt senest 72 timer,* efter at denne er blevet bekendt med det, anmelde bruddet til Datatilsynet. Foretages anmeldelsen til Datatilsynet ikke inden for 72 timer, ledsages den af en begrundelse for forsinkelsen.

3.3.1 Bekendt med bruddet

Den dataansvarliges forpligtelse til at foretage anmeldelse af et brud på persondatasikkerheden til Datatilsynet aktiveres først, når den dataansvarlige er *blevet bekendt med, at der er sket et brud på persondatasikkerheden*.

Det er i den forbindelse Datatilsynets opfattelse, at en dataansvarlig som udgangspunkt anses for at være bekendt med et brud, når en medarbejder hos den dataansvarlige bliver bekendt med bruddet, men alene formodningen om, at et brud på persondatasikkerheden har fundet sted ikke er tilstrækkeligt til at fastslå, at den dataansvarlige er bekendt med et brud.

En formodning om, at der er sket et brud, skal dog føre til, at den dataansvarlige hurtigst muligt undersøger hændelsen med henblik på at afklare, om der rent faktisk er sket et brud på persondatasikkerheden, herunder inddrager alle relevante parter såsom medarbejdere, databehandlere, leverandører, samarbejdspartnere mv.

Det forventes, at den indledende undersøgelse med en rimelig grad af sikkerhed fastslår, om et brud har fundet sted, og den dataansvarlige skal i den forbindelse sikre sig, at alle medarbejdere i organisationen i nødvendigt omfang er bekendt med interne procedurer for håndtering af brud på persondatasikkerheden, og at relevante medarbejdere kan identificere, håndtere og vurdere brud på persondatasikkerheden.

I øvrigt kan formodningen om, at der er sket et brud på persondatasikkerheden, der skal undersøges og anmeldes, både stamme fra den dataansvarlige selv, men den dataansvarlige bør også undersøge alle underretninger om mulige brud, der stammer fra f.eks. databehandlere, samarbejdspartnere, leverandører, registrerede, medierne eller andre kilder.

Hvis den dataansvarlige efter indledende undersøgelser stadig er i tvivl om, at der er sket et brud på persondatasikkerheden, men ikke kan afvise, at det er tilfældet, bør tvivlen som udgangspunkt føre til, at den dataansvarlige anmelder hændelsen som et brud på persondatasikkerheden til Datatilsynet.

Hvis den dataansvarlige efterfølgende bliver bekendt med, at der alligevel ikke var tale om et brud på persondatasikkerheden, kan den dataansvarlige altid kommunikere dette til Datatilsynet.

Hvis den dataansvarlige efter hurtige, indledende undersøgelser har en rimelig grad af vished om, at der er sket et brud på sikkerheden, der kompromitterer personoplysninger, vil den

dataansvarlige som udgangspunkt være bekendt med bruddet, og skal herefter anmelde bruddet til Datatilsynet hurtigst muligt og senest inden for 72 timer, med mindre, at det er usandsynligt, at bruddet indebærer en risiko for de berørte.

Eksempler på situationer, hvor en dataansvarlig anses for at være bekendt/ikke bekendt med et brud, fremgår af EDPBs retningslinjer om anmeldelse af brud på persondatasikkerheden[5] side 11 ff.

3.3.2 Uden unødig forsinkelse

En anmeldelse om et brud på persondatasikkerheden skal ske *uden unødig forsinkelse og om muligt senest 72 timer efter den dataansvarlige er blevet bekendt med det*.

Den dataansvarlige er dermed forpligtet til at anmelde bruddet til Datatilsynet, så snart det er muligt – også selv om dette tidspunkt indtræder før udløbet af de 72 timer.

Når Datatilsynet vil skulle fastslå, hvorvidt en anmeldelse har fundet sted *uden unødig forsinkelse* – efter at den dataansvarlige er blevet bekendt med bruddet – vil det ske under særlig hensyntagen til karakteren og alvoren af bruddet på persondatasikkerheden og dets konsekvenser og skadevirkninger for den registrerede.

Hvis der er tale om et alvorligt brud på persondatasikkerheden, som endnu ikke er standset, og hvor der er risiko for yderligere kompromittering af personoplysninger, vil den dataansvarlige formentlig kunne retfærdiggøre en vis forsinkelse i anmeldelsen, hvis forsinkelsen skyldes den dataansvarliges bestræbelser på at standse bruddet og minimere dets skadevirkninger.

Tilsvarende må en vis forsinkelse kunne forsvares i tilfælde af, at den dataansvarlige er bekendt med, at personoplysninger er blevet tilgået af personer, der har til hensigt at misbruge disse til kriminelle formål, og den dataansvarlige derfor i første omgang prioriterer at få forhindret dette, f.eks. ved at gå i dialog med Styrelsen for Samfundssikkerhed og/eller politiet.

Tidsfristen på de 72 timer skal i øvrigt overholdes uanset, om den dataansvarlige først bliver bekendt med bruddet uden for normal kontortid, herunder i weekender og på helligdage.

Det er i den forbindelse Datatilsynets opfattelse, at manglende anmeldelse af brud inden for 72 timer generelt ikke kan begrundes med, at personale, der almindeligvis er medansvarlig for anmeldelse af brud på persondatasikkerheden ikke er til stede – f.eks. pga. ferie eller sygdom – da det må forventes, at den dataansvarlige har taget højde herfor ved etablering af passende procedurer, beredskabsplaner og lignende.

Tidsfristen på 72 timer skal som udgangspunkt også overholdes, selvom det ikke er muligt for den dataansvarlige at lave en fyldestgørende anmeldelse af bruddet på persondatasikkerheden inden for tidsfristen. I så fald skal den dataansvarlige lave en så fyldestgørende anmeldelse som muligt inden for tidsfristen, og efterfølgende oplysninger om bruddet skal herefter meddeles trinvist uden unødig yderligere forsinkelse. Se nærmere herom under afsnit 3.6. nedenfor.

Hvis den dataansvarlige anmelder et brud på persondatasikkerheden efter udløbet af fristen på 72 timer, skal anmeldelsen ledsages af en begrundelse for forsinkelsen. Datatilsynet vil i den forbindelse altid vurdere, om begrundelsen retfærdiggør forsinkelsen, og vil kunne gøre brug af sine sanktionsbeføjelser, hvis det ikke er tilfældet.

Relevante bestemmelser mv.

- Forordningens artikel 33, stk. 1 og 4
- Præambelbetragtning nr. 85

[5] Retningslinjer 9/2022 om anmeldelse af brud på persondatasikkerheden i henhold til GDPR

3.4 Hvem skal anmelde til Datatilsynet?

Som udgangspunkt er det den dataansvarlige, der skal anmelde et brud på persondatasikkerheden til Datatilsynet.

Den dataansvarlige bør i den forbindelse udpege en eller flere medarbejdere i organisationen, som er bemyndiget til at anmelde brud på persondatasikkerheden til Datatilsynet på vegne af den dataansvarlige. Dette kan med fordel være en person, som i forvejen i kraft af sin stilling vil være involveret i håndteringen af brud på persondatasikkerheden hos den dataansvarlige.

En databehandler vil også kunne anmelde et brud på persondatasikkerheden til Datatilsynet på vegne af den dataansvarlige. Dette forudsætter imidlertid, at databehandleren har fået bemyndigelse hertil (fuldmagt). Ligeledes vil andre parter – som f.eks. advokater eller konsulenter – kunne anmelde brud på vegne af den dataansvarlige, hvis de er bemyndiget til det.

Det overordnede juridiske ansvar for at anmelde et brud på persondatasikkerheden – herunder at dette sker rettidigt – forbliver dog altid hos den dataansvarlige, uanset om den dataansvarlige har bemyndiget andre til at foretage anmeldelse på vegne af sig.

Relevante bestemmelser mv.

- Forordningens artikel 33, stk. 1
- Præambelbetragtning nr. 85

3.5 Hvilke forpligtelser har databehandleren?

Bliver en databehandler opmærksom på, at der er sket et brud på persondatasikkerheden, har databehandleren pligt til uden unødig forsinkelse at underrette den eller de dataansvarlige om bruddet, hvis bruddet på persondatasikkerheden omfatter personoplysninger, som den eller de dataansvarlige er ansvarlig for.

Der er tale om en forpligtelse, som databehandleren skal efterleve i alle tilfælde. Databehandleren kan f.eks. ikke undlade at underrette den dataansvarlige om et brud på persondatasikkerheden med henvisning til, at databehandleren selv har vurderet, at det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Der skal også ske underretning af den dataansvarlige uanset, at databehandleren har en formodning om, at den dataansvarlige allerede er bekendt med bruddet.

Databehandleren bør straks underrette den dataansvarlige og herefter følge op med den information vedrørende bruddet, som løbende bliver tilgængelig for databehandleren. Dette er bl.a. afgørende for, at den dataansvarlige kan efterleve kravet om anmeldelse til Datatilsynet inden for 72 timer. Databehandlerens pligt til – og procedure for – at underrette den dataansvarlige om et brud på persondatasikkerheden bør derfor fremgå af databehandleraftalen mellem den dataansvarlige og databehandleren.

Hvis databehandleren er databehandler for flere dataansvarlige, som alle er berørt af det samme brud på persondatasikkerheden, skal databehandleren underrette hver dataansvarlig individuelt.

En databehandler kan også anmelde brud på vegne af en dataansvarlig, men er ikke forpligtet til det, jf. afsnit 3.4 ovenfor.

Relevante bestemmelser mv.

- Forordningens artikel 28, stk. 3, litra f og artikel 33, stk. 2

3.6 Hvilke oplysninger skal gives til Datatilsynet?

Når en dataansvarlig anmelder et brud på persondatasikkerheden til Datatilsynet, skal anmeldelsen *som minimum*:

- 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
- angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
- 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.

Oplysningerne bør så vidt muligt gives på en måde, så omstændighederne ved bruddet kan forstås og vurderes af personer, der ikke nødvendigvis har kendskab til den dataansvarliges myndigheds- eller forretningsområde.

De oplysninger, anmeldelsen som minimum skal indeholde, skal bidrage til, at Datatilsynet får mulighed for at følge og vurdere, at håndteringen af bruddet på persondatasikkerheden hos den dataansvarlige sker på en hensigtsmæssig måde. Datatilsynet kan også anvende oplysningerne i forbindelse med vurderingen af, hvorvidt der er behov for, at tilsynet træffer en afgørelse i forhold til spørgsmålet om underretning af de registrerede, hvis dette endnu ikke er sket, eller hvis tilsynet overvejer at gøre brug af sine korrigerende beføjelser til midlertidigt eller definitivt at begrænse eller forbyde en behandling af personoplysninger.

Datatilsynet kan kræve yderligere oplysninger af den dataansvarlige, hvis det er nødvendigt for, at tilsynet kan vurdere omstændighederne ved bruddet og behandle en eventuelt efterfølgende sag.

Anmeldelsesblanketten – jf. afsnit 3.1 – vejleder i høj grad den dataansvarlige til at afgive nødvendige oplysninger, hvorfor blanketten bør anvendes, så kravene i loven så vidt muligt overholdes, samtidig med, at sandsynligheden for en hurtig, effektiv behandling af anmeldelsen af bruddet på persondatasikkerheden hos Datatilsynet øges.

Relevante bestemmelser mv.

- Forordningens artikel 33, stk. 3, litra a-d

3.7 Situationer, hvor anmeldelse til Datatilsynet ikke er nødvendigt

Et brud på persondatasikkerheden skal ikke anmeldes til Datatilsynet, hvis det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

At et brud på persondatasikkerheden vurderes til ikke at ville få konsekvenser for de berørte personer kan f.eks. skyldes de sikkerhedsforanstaltninger, som er truffet af den dataansvarlige. Det kan dog også skyldes den dataansvarliges hurtige indgriben eller mulighed for at konstatere, om personoplysninger er kommet til uvedkommendes kendskab.

Det er den dataansvarlige, som har bevisbyrden for, at der foreligger omstændigheder, der gør, at det er usandsynligt, at et brud på persondatasikkerheden har eller kan få konsekvenser for de berørte personer.

At kunne bevise, at bruddet ikke indebærer konsekvenser for de registrerede, betyder, at man skal have afdækket alle muligheder for, at bruddet kan have eller have haft konsekvenser for de registrerede.

Hvis der f.eks. har været uautoriseret adgang til oplysninger i en organisations it-miljø, så skal den dataansvarlige kunne bevise – herunder ved brug af tekniske foranstaltninger – at den uautoriserede adgang ikke har været udnyttet af uvedkommende.

Det kan f.eks. være, hvis:

- der er troværdige logs, som registrerer alles adgang til disse data, og
- disse logs dækker hele perioden for den uautoriserede adgang, og
- den dataansvarlige ved, at logs ikke er blevet manipuleret, og
- disse logs viser, at der ikke er uautoriserede personer, der har tilgået data, mens der var adgang til dem.

Er det ikke muligt for den dataansvarlige at undersøge mulige konsekvenser indenfor 72 timer – som er tidsfristen for at anmelde bruddet til Datatilsynet – vil det normalt indebære, at det ikke kan vurderes, om det er usandsynligt, at bruddet indebærer en risiko for de berørte registrerede. I sådanne situationer vil man som udgangspunkt skulle anmelde bruddet på persondatasikkerheden til Datatilsynet.

Det er vigtigt at understrege, at den dataansvarlige ved en vurdering af risikoen for de berørte personers rettigheder skal tage alle omstændighederne ved det pågældende brud i betragtning.

3.8 Eksempler

Det Europæiske Databeskyttelsesråd (EDPB) har – med involvering af det danske datatilsyn – udarbejdet et sæt retningslinjer[6] med en række eksempler på brud på persondatasikkerheden, hvor det vurderes, om et brud på persondatasikkerheden kræver anmeldelse.

Eksemplerne kan findes på EDPBs hjemmeside. EDPB har også udarbejdet et sæt retningslinjer om anmeldelse af brud på persondatasikkerheden i henhold til GDPR[7], hvori der kan findes yderligere vejledning og eksempler.

Retningslinjerne fra EDPB vil altid kunne findes på Datatilsynets hjemmeside sammen med denne vejledning.

3.9 Hvis bruddet indebærer en risiko for registrerede i flere lande

Ved grænseoverskridende behandlinger af personoplysninger kan et brud på persondatasikkerheden indebære en risiko for fysiske personers rettigheder og frihedsrettigheder i mere end ét EU/EØS[8]-medlemsland.

En dansk virksomhed kan f.eks. behandle oplysninger om fysiske personer, der befinder sig i andre EU/EØS-medlemslande. Der findes også virksomheder i Danmark, som udelukkende behandler oplysninger om fysiske personer, der befinder sig i andre EU/EØS-medlemslande.

Der gælder i sådanne situationer de samme betingelser for, hvornår et brud på persondatasikkerheden skal anmeldes til tilsynsmyndigheden, men hvilken tilsynsmyndighed i EU/EØS, der er kompetent til at behandle anmeldelsen er ikke i alle tilfælde Datatilsynet i Danmark.

Den kompetente myndighed er tilsynsmyndigheden i det land, hvor hovedvirksomheden ligger, eller det land, hvor den del af virksomheden, der træffer alle beslutninger om virksomhedens behandling af personoplysninger, er placeret. Den kompetente tilsynsmyndighed kaldes her også for den ledende tilsynsmyndighed[9].

Når et brud på sikkerheden omhandler oplysninger om fysiske personer i mere end ét EU/EØS-medlemsland, og der skal ske anmeldelse, er den dataansvarlige kun forpligtet til at foretage anmeldelse til den ledende tilsynsmyndighed.

---

[6] Retningslinjer 01/2021 om eksempler af brud på persondatasikkerheden

[7] Retningslinjer 9/2022 om anmeldelse af brud på persondatasikkerheden i henhold til GDPR

[8] EØS er forkortelsen for Det Europæiske Økonomiske Samarbejdsområde, som ud over EU-medlemslandene består af Norge, Island og Liechtenstein.

[9] Se i den forbindelse også Retningslinjer 08/2022 for udpegelse af en ledende tilsynsmyndighed for en dataansvarlig eller databehandler (WP 244 rev.01).

Det er en fordel for virksomheden, hvis den – efter at have udpeget, hvilken tilsynsmyndighed, der er ledende tilsynsmyndighed for virksomheden – sørger for at skrive det ind i virksomhedens procedure for håndtering af brud på persondatasikkerheden. På den måde sikres det, at den dataansvarlige ikke skal bruge tid på at foretage denne vurdering, når/hver gang der sker et brud på persondatasikkerheden.

Hvis den dataansvarlige indenfor 72 timer fra bruddet er konstateret ikke har nået at fastlægge, hvem der er ledende tilsynsmyndighed for virksomheden – eller er i tvivl om, hvorvidt vurderingen er korrekt – skal bruddet anmeldes til den "lokale" tilsynsmyndighed i det EU/EØS-land, hvor bruddet på persondatasikkerheden er sket, eller som bruddet på persondatasikkerheden berører.

Det kan også være, at en dataansvarlig af sig anmelder et brud på persondatasikkerheden til en tilsynsmyndighed, som virksomheden er vidende om ikke er ledende tilsynsmyndighed for den dataansvarlige, f.eks. hvis den dataansvarlige ved, at der er fysiske personer i dette pågældende EU-medlemsland, der er berørt af bruddet.

Når den dataansvarlige anmelder et brud på persondatasikkerheden til den ledende tilsynsmyndighed, skal den dataansvarlige oplyse til tilsynsmyndigheden i hvilke EU/EØS-medlemslande, der er fysiske personer, som er berørt af bruddet.

Når den ledende tilsynsmyndighed – f.eks. Datatilsynet i Danmark – har modtaget anmeldelsen, herunder oplysningerne om, at fysiske personer i andre EU/EØS-medlemslande er berørt af et brud på persondatasikkerheden, er det den ledende tilsynsmyndigheds ansvar at underrette de relevante tilsynsmyndigheder i de respektive medlemslande, hvis det vurderes nødvendigt i forbindelse med behandlingen af anmeldelsen.

Eksempel 18: Tilsynsmyndighed

En virksomhed med hovedvirksomhed i Danmark tilbyder via sin hjemmeside onlinesalg af håndkøbsmedicin. Ved en fejl kommer virksomheden til på hjemmesiden at offentliggøre en oversigt over virksomhedens seneste onlinesalg. Oversigten indeholder kundernes fulde navn, ligesom der fremgår bl.a. betalings-, kontakt- og adresseoplysninger på kunderne. Virksomheden har kunder i Danmark, men en del af kunderne befinder sig i andre EU/EØS-medlemslande, og ud fra den offentliggjorte oversigt kan virksomheden konstatere, at et antal kunder er bosat i Spanien, Sverige og Tyskland har været berørt af lækagen.

Virksomheden vurderer, at dette brud på persondatasikkerheden skal anmeldes, og den foretager derfor en anmeldelse til Datatilsynet i Danmark. På anmeldelsesblanketten sørger virksomheden for at markere, at personer i de ovenfor angivne EU-medlemslande har været berørt.

Datatilsynet underretter tilsynsmyndighederne i Spanien, Sverige og Tyskland, hvis nødvendigt.

Relevante bestemmelser mv.

- Forordningens artikel 4, nr. 23, artikel 55, stk. 1, artikel 56, stk. 1 og stk. 6
- Præambelbetragtning nr. 122

4. Underretning af den registrerede

4.1 Hvilke brud på persondatasikkerheden kræver underretning?

Når et brud på persondatasikkerheden *sandsynligvis* vil indebære en *høj risiko for fysiske personers rettigheder og frihedsrettigheder* skal den dataansvarlige ikke alene foretage en anmeldelse til Datatilsynet, men også underrette den registrerede om bruddet.

Underretningsforpligtelsen indtræder derfor kun, når et brud *sandsynligvis* indebærer en *høj risiko*, og ikke – som det er tilfældet med anmeldelsespligten til Datatilsynet – i tilfælde, hvor det ikke er *usandsynligt,* at bruddet indebærer en risiko.

Hvis den dataansvarlige ikke underretter de registrerede, har Datatilsynet mulighed for at påbyde den dataansvarlige at foretage korrekt underretning og i øvrigt gøre brug af andre korrigerende beføjelser.

Det grundlæggende formål med underretningsforpligtelsen er bl.a. at give den registrerede mulighed for at træffe de fornødne forholdsregler for at minimere risikoen for sine rettigheder og frihedsrettigheder, når der er sket kompromittering af vedkommendes personoplysninger.

Eksempler på konsekvenser er nævnt tidligere under afsnit 3.2.4 og nedenfor under afsnit 4.3.3, og man skal huske, at konsekvenserne kan komme langt ude i fremtiden selvom bruddet er standset. Hvis bruddet har stået på længe, kan konsekvenserne allerede have manifesteret sig tidligere, og selv i den situation kan det være relevant for de berørte at blive underrettet om bruddet.

Der findes i databeskyttelsesforordningen ikke en definition af begrebet ”høj risiko”. Som tidligere nævnt under afsnit 3.2, består risiko af en *sandsynlighed* for et negativt udfald og en *konsekvens/alvor* ved det negative udfald, der til sammen bestemmer størrelsen af risikoen. Der kan i den forbindelse også være høj risiko i tilfælde, hvor sandsynligheden er lav, men konsekvensen er meget høj. Man skal som dataansvarlig foretage risikovurderingen for de registrerede ud fra de samme kriterier, som der fremgår under afsnit 3.2, med den modifikation, at risikoen *sandsynligvis* skal være *høj*, før underretningsforpligtelsen indtræder.

Når den dataansvarlige skal foretage risikovurderingen, skal alle aktuelle og fremtidige negative konsekvenser for den registrerede tages i betragtning. Dette omfatter således også de eventuelt ”sekundære” konsekvenser for de registrerede, som et brud på persondatasikkerheden kan medføre, herunder hvis f.eks. registreredes brugernavne og/eller kodeord er blevet kompromitteret, og der er en mulighed for, at de registrerede genbruger disse brugernavne og/eller kodeord til andre tjenester, som den dataansvarlige ikke (nødvendigvis) er bekendt med.

Hvis risikoen sandsynligvis kun er høj for en (mindre) andel af de berørte registrerede, så skal den dataansvarlige foretage underretning af disse registrerede, uanset om underretningsforpligtelsen muligvis ikke er indtrådt i forhold til alle registrerede, der er berørt af bruddet.

Læs mere om eksempler på, hvornår der skal ske underretning af registrerede i afsnit 4.7 nedenfor.

4.2 Hvornår skal underretning ske?

Der gælder ikke – som det er tilfældet for anmeldelsespligten, hvor tidsfristen er 72 timer – en specifik tidsfrist for, hvornår en dataansvarlig skal foretage underretning af registrerede.

Den dataansvarlige skal imidlertid underrette den registrerede *uden unødig forsinkelse* efter, at bruddet på persondatasikkerheden er konstateret[10]. Det skal ses i sammenhæng med, at underretningen skal give den registrerede mulighed for at træffe de fornødne forholdsregler til at beskyttes sig selv mod konsekvenser af bruddet, og afhængigt af situationen, kan det dreje som om meget kort tid. Eksempelvis kan oplysninger om adgangskoder og beskyttede fysiske adresser udnyttes meget hurtigt med meget alvorlig konsekvens, så som økonomisk kriminalitet og partnervold.

Derudover vil underretning af registrerede ved brud på persondatasikkerheden, hvor ondsindede aktører som f.eks. hackere er kommet i besiddelse af personoplysninger, som det klare udgangspunkt skulle foretages tilnærmelsesvis straks efter bruddets konstatering, idet formodningen må være, at de ondsindede aktører har til hensigt at misbruge oplysningerne.

Tidspunktet for underretning kan også afhænge af, om den dataansvarlige samarbejder med andre myndigheder – f.eks. politiet eller Styrelsen for Samfundssikkerhed – for at håndtere bruddet på persondatasikkerheden. I sådanne tilfælde vil den dataansvarlige kunne lægge vægt på den vejledning, som den dataansvarlige modtager fra myndighederne – herunder Datatilsynet – når den dataansvarlige skal fastsætte tidspunktet for underretning.

Underretning afhænger i øvrigt nødvendigvis ikke af, hvornår der skal ske anmeldelse af bruddet til Datatilsynet.

Relevante bestemmelser mv.

- Forordningens artikel 34, stk. 1
- Præambelbetragtning nr. 86

4.3 Hvilke oplysninger skal indgå i en underretning?

Underretningen af den registrerede skal i et klart og forståeligt sprog beskrive karakteren af bruddet på persondatasikkerheden og mindst indeholde følgende oplysninger:

- navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
- en beskrivelse af de sandsynlige konsekvenser af bruddet på persondatasikkerheden
- en beskrivelse af 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.

Nedenfor følger en gennemgang af de oplysninger, som en underretning skal indeholde.

4.3.1 Kontaktoplysninger

Underretninger skal først og fremmest indeholde navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor den registrerede kan indhente yderligere oplysninger om bruddet mv.

4.3.2 Beskrivelse af karakteren af bruddet i et klart og forståeligt sprog

Hvis det skal være muligt for den registrerede at træffe de fornødne forholdsregler, skal karakteren af bruddet beskrives i et klart og forståeligt sprog. Hvad der udgør et klart og forståeligt sprog skal ses i lyset af det pågældende bruds karakter, og der bør i den sammenhæng tages hensyn til modtageren, heriblandt den registreredes modersmål, sprogkundskaber, alder mv.

Beskrivelsen af karakteren af bruddet skal gøre den registrerede i stand til konkret at forstå, hvad der er sket med den registreredes oplysninger, f.eks. om den registreredes oplysninger

[10] For nærmere beskrivelse af, hvornår en dataansvarlig anses for at være blevet bekendt med et brud på persondatasikkerheden, henvises til afsnit 3.3.1 ovenfor

er blevet sendt til en forkert modtager, eller om den registreredes oplysninger har været omfattet af et hackerangreb.

Det vil i den forbindelse ikke være tilstrækkeligt, hvis det kun fremgår af underretningen, at oplysningerne er kommet til uvedkommendes kendskab. Det bør endvidere beskrives, hvordan oplysningerne er kommet til uvedkommendes kendskab, herunder om der f.eks. er tale om fejlforsendelse ved fysisk brev, eller om en e-mail er sendt til en eller flere forkerte modtagere. Hvis oplysningerne har været omfattet af et hackerangreb, bør en beskrivelse af karakteren af bruddet – hvis det er muligt – også omfatte en beskrivelse af, om oplysningerne f.eks. er blevet gjort utilgængelige hos den dataansvarlige og/eller er blevet offentliggjort på internettet.

For at den registrerede kan vurdere, hvordan vedkommende bedst kan varetage sine interesser, kan det i nogle tilfælde være relevant at oplyse den pågældende om, hvem – og hvor mange – der utilsigtet har modtaget den registreredes oplysninger.

Det indebærer imidlertid ikke, at den dataansvarlige f.eks. skal oplyse navnet på en borger, der utilsigtet har modtaget oplysninger om den registrerede. Det kan dog ofte være relevant for den registrerede at få oplyst, om den utilsigtede modtager er en anden borger, en kollega, et familiemedlem eller lignende, eller om den utilsigtede modtager f.eks. er en advokat, der i øvrigt er underlagt tavshedspligt.

Øvrige oplysninger, såsom personoplysningernes art, følsomhed og mængde, er som regel også væsentlige og relevante for den registrerede at få kendskab til. Det indebærer bl.a., at den dataansvarlige i underretningen både beskriver, hvilke kategorier af oplysninger – f.eks. helbredsoplysninger eller økonomiske oplysninger – der er omfattet af bruddet, samt præciserer, hvilke konkrete oplysninger der er omfattet. Det kan eksempelvis være helbredsoplysninger i form af oplysninger om diagnose og medicinering i en lægejournal.

I forbindelse med en underretning af den registrerede, vil det i visse tilfælde være hensigtsmæssigt at vedlægge de konkrete dokumenter, oplysninger eller lignende, der har været omfattet af bruddet.

Det er imidlertid Datatilsynets opfattelse, at en underretning skal kunne stå alene, idet der kan være en risiko for, at den registrerede ikke læser eventuelle vedlagte dokumenter, f.eks. hvis dokumenterne er sendt i et filformat, som ikke er læsbart for den registrerede. Der kan derudover være en risiko for, at det ud fra de vedlagte dokumenter ikke er klart for den registrerede, om der f.eks. er tale om særlige kategorier af oplysninger (f.eks. helbredsoplysninger), hvilket kan medføre, at den registrerede ikke kan vurdere risikoen ved det pågældende brud. Indholdet af eventuelle vedlagte dokumenter bør derfor uddybes i selve underretningsskrivelsen.

Endelig bør journalnumre, datoer, titler mv. på dokumenter, der er omfattet af et brud – hvis det er hensigtsmæssigt – angives, så den registrerede i videst mulige omfang har mulighed for at identificere de konkrete dokumenter og oplysninger, der er omfattet af bruddet. Dette gælder især i tilfælde af, at disse ikke er vedlagt i underretningen.

4.3.3 Beskrivelse af sandsynlige konsekvenser

Underretningen skal herudover indeholde en klar og forståelig beskrivelse af de sandsynlige konsekvenser af bruddet for den registrerede, for at sikre, at den registrerede kan tage passende forholdsregler for at minimere risikoen. Det betyder, at det ikke er tilstrækkeligt alene at oplyse en delmængde af de sandsynlige konsekvenser, men at samtlige sandsynlige konsekvenser skal beskrives.

Hvis et brud f.eks. består i, at personoplysninger om den registrerede utilsigtet er blevet videregivet til uvedkommende, skal den dataansvarlige beskrive, hvad de sandsynlige konsekvenser af bruddet på fortroligheden kan være, f.eks. identitetstyveri eller lignende. Det er ikke tilstrækkeligt alene at beskrive, at oplysninger f.eks. kan tilgås af uvedkommende, er blevet ændret eller er gået tabt mv. Det er også konsekvenserne af, at oplysninger f.eks. er gået tabt, der skal beskrives.

Databeskyttelsesforordningen beskriver en række eksempler på sandsynlige konsekvenser.

Der kan f.eks. være tale om:

- Fysisk skade
- Materiel skade
- Immateriel skade
- Forskelsbehandling
- Identitetstyveri
- Identitetssvig
- Økonomiske konsekvenser, herunder finansielle tab
- Skade på omdømme
- Sociale konsekvenser
- Indflydelse på privatliv
- Skade på menneskelig værdighed
- Skade på legitime interesser
- Begrænsning/krænkelse af fundamentale rettigheder og frihedsrettigheder
- Manglende udøvelse af kontrol med egne personoplysninger.

I et tilfælde, hvor personoplysninger – herunder fulde navn, adresse og helbredsoplysninger – i en livsforsikring er blevet tilgået af uvedkommende, kunne en beskrivelse af de sandsynlige konsekvenser til illustration være:

- Offentliggørelse af oplysninger om den registrerede på internettet, som f.eks. kan påvirke den registreredes mulighed for at finde et arbejde eller lignende (på baggrund af oplysninger om helbredsproblemer, graviditet mv.)
- Følelsesmæssig påvirkning af den registrerede, hvis den registrerede skjuler sin diagnose
- Identitetstyveri
- Oplysningerne kan blive udnyttet til phishing.

Hvornår en sandsynlig konsekvens er tilstrækkeligt beskrevet, afhænger af en konkret vurdering. Det afgørende er, at den sandsynlige konsekvens er forståelig og detaljeret nok beskrevet til, at den registrerede får mulighed for at tage korrekte forholdsregler.

4.3.4 Beskrivelse af foranstaltninger

Underretningen skal endvidere indeholde en beskrivelse af 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. Hvis den dataansvarlige ikke har fundet det relevant at træffe foranstaltninger på baggrund af bruddet, skal dette efter Datatilsynets opfattelse fremgå af underretningen.

Hvis det er relevant for den registrerede, bør underretningen også indeholde oplysninger om de foranstaltninger, som den dataansvarlige eventuelt har truffet for at undgå nye lignende brud. Det er i den forbindelse Datatilsynets opfattelse, at det kan være hensigtsmæssigt at oplyse en registreret, der har været berørt af et brud, om, at den dataansvarlige f.eks. har indskærpet retningslinjer over for medarbejdere, gennemført yderligere awareness mv. og/eller etableret yderligere tekniske sikkerhedsforanstaltninger som følge af bruddet, idet oplysningerne kan gøre den registrerede bedre i stand til at vurdere, om den dataansvarlige behandler den registreredes oplysninger tilstrækkeligt sikkert fremadrettet, eller om den registrerede f.eks. vil tilbagekalde sit samtykke til behandlingen, opsige/ophæve en kontrakt eller gøre brug af retten til sletning, hvis det er muligt. Oplysningerne skal imidlertid ikke være så detaljerede, at den dataansvarlige f.eks. afslører sårbarheder i it-systemer eller lignende.

Endelig vil det også være relevant at oplyse den registrerede om, hvorvidt en eventuel forkert modtager af den registreredes oplysninger er blevet anmodet om at slette de modtagne oplysninger, og om modtageren har bekræftet, at oplysningerne er blevet slettet.

4.3.5 Anbefalinger og specifikke råd til den registrerede

Foruden en beskrivelse af de sandsynlige konsekvenser skal underretningen i relevant omfang indeholde anbefalinger eller specifikke råd til den registrerede med henblik på at begrænse de mulige skadevirkninger af bruddet.

Det indebærer f.eks., at hvis en streamingtjeneste er blevet hacket, og hackeren bl.a. har fået adgang til og/eller offentliggjort den registreredes brugernavn og adgangskode til tjenesten, skal underretningen indeholde anbefaling om, at den registrerede bør bruge forskellige adgangskoder på forskellige websteder og samtidig bør ændre adgangskoderne til konti, hvor den kompromitterede adgangskode blev anvendt.

4.3.6 Opfølgende underretning

Der kan efter Datatilsynets opfattelse være situationer, hvor en opfølgende underretning af den/de registrerede vil være hensigtsmæssig. Det kan f.eks. være, hvis den dataansvarlige som led i afdækningen af et brud på persondatasikkerheden bliver bekendt med nye forhold, der er af betydning for den registrerede, efter den dataansvarlige allerede har foretaget underretning.

Det vil eksempelvis være formålstjenligt at foretage opfølgende underretning af berørte registrerede, hvis den dataansvarlige i forbindelse med behandlingen af et brud på persondatasikkerheden, der skyldes et hackerangreb, bliver bekendt med nye oplysninger, der medfører, at risikoen for de berørte registreredes rettigheder er højere eller lavere end, hvad den dataansvarlige oprindeligt vurderede. Det kan f.eks. være tilfældet, hvis den dataansvarlige gennem en efterfølgende undersøgelse af bruddet konstaterer, at andre eller flere typer personoplysninger er omfattet af bruddet, end den dataansvarlige først antog. Ved en opfølgende underretning får den registrerede en mere præcis opfattelse af bruddets karakter og de konkrete risikoscenarier mv., så den registrerede eventuelt kan træffe yderligere forholdsregler for at beskytte sine rettigheder og frihedsrettigheder.

Dataansvarlige skal imidlertid altid underrette registrerede uden unødig forsinkelse. Formålet med en opfølgende underretning af registrerede medfører derfor ikke, at dataansvarlige kan undlade at underrette registrerede så hurtigt som muligt efter bruddets konstatering ved brug af de informationer, som er tilgængelige for den dataansvarlige på det tidspunkt.

4.4 Hvordan skal den registrerede underrettes

Der er i databeskyttelsesforordningen ikke fastsat formkrav til, hvordan den registrerede skal underrettes, men det anbefales, at den dataansvarlige vælger den eller de mest hensigtsmæssige underretningsmetoder i forhold til den registrerede. Det er imidlertid fastsat, at underretning af den registrerede som det klare udgangspunkt skal ske direkte og på et skriftligt grundlag, f.eks. via e-mail, brev, sms eller lignende. En underretning, der begrænser sig til en pressemeddelelse eller et opslag i en virksomheds blog vil typisk ikke være tilstrækkelig. Meddelelsen til den registrerede må heller ikke sendes til vedkommende sammen med anden information, så som generelle opdateringer, nyhedsbreve eller standardmeddelelser fra den dataansvarlige.

Det er i den forbindelse Datatilsynets opfattelse, at underretning i nogle tilfælde kan ske mundtligt – f.eks. ved et telefonopkald – men at dette som udgangspunkt kun kan ske, hvis den registreredes helt særlige forhold – f.eks. helbred – tilsiger det. Det kan f.eks. være, hvis den registrerede har et synshandicap eller lignende, der medfører, at den registrerede har svært ved at få adgang til eller forstå oplysninger i skriftlig form. Det kan også være, hvis den registrerede selv anmoder om det.

Man skal imidlertid have for øje, at det ofte ved underretninger om brud på persondatasikkerheden er den dataansvarlige, der retter henvendelse til den registrerede (og ikke omvendt, som det typisk er tilfældet, hvis den registrerede ønsker at udøve sine rettigheder til f.eks. indsigt), hvorfor man som dataansvarlig skal være opmærksom på, om den registrerede faktisk anmoder om, at oplysningerne gives mundtligt frem for på skriftligt grundlag. Der er dog intet til hinder for – og det kan i flere tilfælde være det mest hensigtsmæssige – at den dataansvarlige indledningsvist underretter mundtligt i kombination med en opfølgende skriftlig underretning.

4.5 Hvem kan foretage underretning af de registrerede

Det er den dataansvarlige, der har ansvaret for at underrette de berørte personer om et brud på persondatasikkerheden, men den dataansvarlige kan uddelegere opgaven til en

databehandler eller tredjemand. Dette forudsætter imidlertid, at databehandleren eller tredjemand er blevet bemyndiget hertil, f.eks. på baggrund af en fuldmagt. Når det gælder databehandleren, bør denne forpligtelse til at foretage underretning af de registrerede også fremgå af den databehandleraftale, der er indgået mellem parterne, se også afsnit 3.5.

Det overordnede juridiske ansvar for, at der er foretaget underretning af de registrerede, forbliver hos den dataansvarlige, uanset om den dataansvarlige har bemyndiget databehandleren eller tredjemand til at forestå underretningen.

Relevante bestemmelser mv.

- Forordningens artikel 34, stk. 2
- Forordningens artikel 12, stk. 1

4.6 Situationer, hvor der ikke er krav om underretning

Det er ikke nødvendigt at foretage underretning, hvis bruddet på persondatasikkerheden *sandsynligvis* ikke indebærer en *høj* risiko for fysiske personers rettigheder og frihedsrettigheder. Den dataansvarlige skal i den forbindelse altid være i stand til at begrunde, hvorfor den dataansvarlige ikke har valgt at foretage underretning af den registrerede, så Datatilsynet på anmodning kan vurdere, om den dataansvarlige har vurderet risikoen korrekt. Derfor bør (risiko)vurderingen af, hvorfor der ikke blev foretaget underretning altid være dokumenteret.

Herudover er det ikke nødvendigt at underrette den registrerede (direkte) i de fire følgende tilfælde. Den dataansvarlige skal i den forbindelse også altid kunne begrunde, hvorfor der i det konkrete tilfælde ikke blev foretaget underretning.

4.6.1 Foranstaltninger før bruddet reducerer risikoen

Det er ikke nødvendigt at iagttage underretningsforpligtelsen, hvis den dataansvarlige *inden bruddet* har gennemført passende *tekniske og organisatoriske beskyttelsesforanstaltninger* i forhold til de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger som f.eks. kryptering, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil.

4.6.2 Foranstaltninger efter bruddet reducerer risikoen

Hvis den dataansvarlige har truffet foranstaltninger *efter bruddet*, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder sandsynligvis ikke længere er reel, vil det heller ikke være nødvendigt at foretage underretning af de registrerede.

Hvis bruddet f.eks. angår en utilsigtet eksponering af personoplysninger på et drev, i en mappe eller lignende, kan den høje risiko typisk reduceres ved at standse bruddet, herunder slette oplysningerne, hvor de ved en fejl er eksponeret, og undersøge adgangen til oplysningerne, herunder ved brug af logs.

Hvis bruddet vedrører mistet, slettet eller ødelagt data, så kan den høje risiko måske reduceres ved at generhverve data, eller ved at ændre på, hvordan data anvendes, så det undgås, at de registrerede lider skade pga. hændelsen.

4.6.3 Underretning kræver en uforholdsmæssig indsats

Den dataansvarlige vil også kunne undlade at underrette de registrerede *direkte*, hvis det i det konkrete tilfælde vil kræve *en uforholdsmæssig indsats*, men der skal i så fald foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Der skal således ske en afvejning af på den ene side betydningen af en sådan underretning for den registrerede, og på den anden side den arbejdsindsats hos den dataansvarlige, der vil være forbundet med en sådan underretning. Eksempelvis vil det – afhængig af en konkret

vurdering – typisk kunne være uforholdsmæssigt for en dataansvarlig at foretage direkte underretning af registrerede, hvis en sådan underretning kræver, at den dataansvarlige skal indhente yderligere personoplysninger.

Som et andet eksempel på et tilfælde, hvor undtagelsen eventuelt kan finde anvendelse, er en situation, hvor en virksomhed har mistet rådigheden over alle kundeoplysninger i forbindelse med, at virksomhedens kundedatabase er blevet ramt af ransomware, og det ikke er muligt for virksomheden at genskabe databasen. Virksomheden er derfor ikke i stand til at underrette de registrerede direkte, fordi virksomheden ikke præcis ved, hvilke personer, der er berørt af bruddet. Virksomheden bliver derfor nødt til at underrette på tilsvarende effektiv vis, f.eks. ved at foretage en offentlig meddelelse. En offentlig meddelelse kan f.eks. gives på den dataansvarliges hjemmeside, udsendes via nyhedsbrev eller lignende, eller gives gennem medierne, hvis situationen kræver det.

Bevisbyrden for, at ovennævnte undtagelse finder anvendelse, påhviler den dataansvarlige. Den dataansvarlige skal således være i stand til at begrunde, hvorfor underretning af den enkelte registrerede kræver en uforholdsmæssig indsats, og at alle de berørte registrerede underrettes på en tilsvarende effektiv måde, f.eks. via offentlig meddelelse.

4.6.4 Underretning kan undlades i henhold til national lovgivning

Efter databeskyttelseslovens § 22 kan underretning undlades, hvis den registreredes interesse i at få kendskab til oplysningerne må vige for afgørende hensyn til enten private interesser – herunder hensynet til den pågældende selv – eller for afgørende hensyn til offentlige interesser, herunder afgørende hensyn til statens sikkerhed, forsvaret, den offentlige sikkerhed og forebyggelse, efterforskning, afsløring eller retsforfølgning af strafbare handlinger.

Ved afvejningen af, om private eller offentlige interesser overstiger hensynet til den registreredes interesser, skal på den ene side indgå den registreredes interesse i at få kendskab til oplysningerne, og på den anden side de afgørende hensyn til offentlige eller private interesser, herunder hensynet til den pågældende selv.

De private og offentlige interesser, som kan indgå i vurderingen, er såvel både den dataansvarliges som tredjemands interesser. Det bemærkes, at underretningsforpligtelsen kun kan undlades, hvis der er en nærliggende fare for, at de private eller det offentliges interesser vil lide skade af væsentlig betydning.

Selve afvejningen af de modstående interesser skal som udgangspunkt foretages for hver enkelt oplysning for sig med den virkning, at man kun må undlade at give den eller de oplysninger om bruddet, som omfattes af de offentlige eller private interesser.

Idet formålet med underretning af registrerede som det klare udgangspunkt er at give den registrerede mulighed for at træffe de fornødne forholdsregler for at minimere risikoen for sine rettigheder og frihedsrettigheder, skal der tungtvejende hensyn til for, at en dataansvarlig kan gøre undtagelse til sin underretningsforpligtelse efter denne bestemmelse. Hvis den dataansvarlige er i tvivl om, at der kan gøres undtagelse til underretningsforpligtelsen, bør tvivlen derfor som udgangspunkt føre til, at den registrerede underrettes.

4.7 Eksempler

Det Europæiske Databeskyttelsesråd (EDPB) har – med involvering af det danske datatilsyn – udarbejdet et sæt retningslinjer[11] med en række eksempler på brud på persondatasikkerheden, hvor det vurderes, om et brud på persondatasikkerheden kræver underretning af de registrerede.

Eksemplerne kan findes på EDPBs hjemmeside. EDPB har også udarbejdet et sæt retningslinjer om anmeldelse af brud på persondatasikkerheden i henhold til GDPR[12], hvori der kan findes yderligere vejledning og eksempler.

[11] Retningslinjer 01/2021 om eksempler af brud på persondatasikkerheden

[12] Retningslinjer 9/2022 om anmeldelse af brud på persondatasikkerheden i henhold til GDPR

Retningslinjerne fra EDPB vil altid kunne findes på Datatilsynets hjemmeside sammen med denne vejledning.

Relevante bestemmelser mv.

- Forordningens artikel 23 og 34, stk. 3
- Præambelbetragtning nr. 88
- Databeskyttelseslovens § 22

4.8 Underretning efter krav fra Datatilsynet

Hvis den dataansvarlige ikke allerede har underrettet den registrerede om bruddet på persondatasikkerheden, kan Datatilsynet efter at have overvejet sandsynligheden for, at bruddet på persondatasikkerheden indebærer en høj risiko, kræve, at den dataansvarlige gør dette. Muligheden for Datatilsynet til at kræve underretning er uafhængig af, om den dataansvarlige er enig med tilsynet.

Situationen kan f.eks. opstå i forbindelse med en anmeldelse af et brud på persondatasikkerheden til Datatilsynet, hvor den dataansvarlige vælger ikke at underrette den registrerede. Hvis Datatilsynet vurderer, at der ikke er tilstrækkelige holdepunkter for den manglende underretning, vil tilsynet – som det klare udgangspunkt efter at have været i dialog med den dataansvarlige – kunne meddele den dataansvarlige, at der skal ske underretning. En sådan meddelelse kan evt. kombineres med et påbud om at foretage underretningen.

Den dataansvarliges (og databehandlerens) manglende efterlevelse af reglerne om underretning af de registrerede kan resultere i, at Datatilsynet f.eks. udtaler kritik. Afhængigt af omstændighederne i hver enkelt sag – herunder hvis en dataansvarlig ikke har fulgt et påbud om underretning fra Datatilsynet – kan der imidlertid også blive tale om at sanktionere den manglende efterlevelse af reglerne med bøde – enten i kombination med eller i stedet for en af Datatilsynets korrigerende beføjelser.

Relevante bestemmelser mv.

- Forordningens artikel 34, stk. 4

5. Ansvarlighed og intern dokumentation

Den dataansvarlige skal dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger.

Det er i den forbindelse uden betydning, om bruddet er af en sådan karakter, at den dataansvarlige er forpligtet til at anmelde det til Datatilsynet – også i de tilfælde, hvor den dataansvarlige har vurderet, at bruddet ikke skal anmeldes, skal den dataansvarlige opbevare disse oplysninger.

Formålet med denne dokumentationspligt er bl.a. at sætte Datatilsynet i stand til at kontrollere, om forpligtelsen i databeskyttelsesforordningen til at anmelde visse brud på persondatasikkerheden er overholdt. Pligten hænger imidlertid også sammen med forordningens princip om ansvarlighed (”accountability”).

Den dataansvarlige har alene pligt til at udlevere dokumentationen til Datatilsynet, hvis tilsynet anmoder herom.

Der er i databeskyttelsesforordningen ikke fastsat specifikke formkrav til dokumentationen, og den dataansvarlige kan derfor selv beslutte, hvordan oplysningerne skal indsamles, og hvordan de skal præsenteres.

Dokumentationen skal imidlertid i alle tilfælde indeholde en række informationer om bruddet, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger. Kravene til dokumentationen kan også opstilles således:

- Dato og tidspunkt for bruddet
- Hvad skete der i forbindelse med bruddet
- Hvad er årsagen til bruddet
- Hvilke (typer) personoplysninger er omfattet af bruddet
- Hvilke konsekvenser har bruddet for de berørte personer
- Hvilke afhjælpende foranstaltninger er truffet
- Hvorvidt der er sket anmeldelse til Datatilsynet eller ej

Den dataansvarlige bør endvidere sørge for at dokumentere sine begrundelser for alle væsentlige beslutninger, der træffes som følge af bruddet. Dette gælder i særdeleshed, hvis den dataansvarlige – efter at have vurderet omstændighederne ved bruddet – er nået frem til, at det ikke skal anmeldes til Datatilsynet. Dokumentationen bør således i relation til denne beslutning omfatte en nærmere redegørelse for, hvorfor den dataansvarlige mener, at bruddet sandsynligvis ikke vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder, hvilket også gælder i forhold til spørgsmålet om underretning af den registrerede. Hvis den dataansvarlige efter at have foretaget en vurdering af bruddet er nået frem til, at en af betingelserne for ikke at skulle underrette er opfyldt, er det vigtigt også at kunne dokumentere, at dette er tilfældet på et senere tidspunkt.

Hvis den dataansvarlige anmelder et brud på persondatasikkerheden til Datatilsynet efter udløbet af fristen på de 72 timer, skal anmeldelsen ledsages af en begrundelse for denne forsinkelse. De oplysninger omkring bruddet, som den dataansvarlige måtte have indsamlet og fortsat opbevarer som følge af pligten til at dokumentere, vil her også kunne bruges til at retfærdiggøre forsinkelsen.

Kopi af en (eventuel) anmeldelse af et brud på persondatasikkerheden til Datatilsynet kan også indgå som en del af dokumentationen. Dette forudsætter selvfølgelig, at anmeldelsesblanketten er udfyldt korrekt og tilstrækkeligt fyldestgørende. Det samme gælder kopi af en (eventuel) underretning til de registrerede.

Det er i øvrigt Datatilsynets opfattelse, at det almindeligvis vil være hensigtsmæssigt at opbevare dokumentationen i en periode på fem år, efter at bruddet har fundet sted, hvilket blandt andet er begrundet i, at forældelsesfristen for overtrædelse af databeskyttelsesforordningen, databeskyttelsesloven eller regler udstedt i medfør heraf – og dermed også tilsynets kontrol af, at en dataansvarlig har håndteret et brud i overensstemmelse med reglerne – er fem år[13].

Til brug for intern dokumentation kan en dataansvarlig tage udgangspunkt i følgende dokumentationsregister:

Brud på persondatasikkerheden hos [navnet på virksomheden/myndigheden]:	Beskrivelse af bruddet:
1. Dato og tidspunkt for bruddet?	
2. Hvad er der sket?	
3. Årsagen til bruddet?	
4. Hvilken type personoplysninger er berørt?	
5. Hvilke konsekvenser har bruddet for de berørte personer?	
6. Hvilke afhjælpende foranstaltninger er truffet?	
7. Er der sket anmeldelse af bruddet til Datatilsynet (hvis ja, hvornår)?	
7.1 Hvis nej, begrundelse for ikke at anmelde bruddet til Datatilsynet?	
8. Er der sket underretning af de berørte personer (hvis ja, hvornår)?	
8.1. Hvis nej, begrundelse for ikke at underrette de berørte personer?	

Relevante bestemmelser mv.

- Forordningens artikel 5, stk. 2 og artikel 33, stk. 5,
- Præambelbetragtning nr. 85

[13] Jf. databeskyttelseslovens § 41, stk. 7

6. Krav om anmeldelse til andre myndigheder i medfør af anden lovgivning

Ved et brud på persondatasikkerheden er det vigtigt at være opmærksom på, at der kan være pligt til at anmelde brud på persondatasikkerheden til andre myndigheder i medfør af anden lovgivning. Du kan læse mere om, hvad der skal indberettes og hvordan du indberetter på de respektive myndigheders hjemmesider.

6.1 Digitaliseringsstyrelsen

Telesektoren og virksomheder, som er omfattet af den særlige telelovgivning, er underlagt en pligt til at underrette **Digitaliseringsstyrelsen** om brud på persondatasikkerheden, jf. § 8 i lov om elektroniske kommunikationsnet og -tjenester[14] og § 5 i bekendtgørelse nr. 1882 af 4. december 2020 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester og nummeruafhængige kommunikationstjenester.

6.2 Styrelsen for Samfundssikkerhed

Alle statslige myndigheder (herunder også kommuner og regioner) er forpligtet til at underrette Center for Cybersikkerhed – nu **Styrelsen for Samfundssikkerhed –** om større sikkerhedshændelser, herunder sikkerhedshændelser, der berører personoplysninger. Herudover kan private dataansvarlige frivilligt anmelde brud på persondatasikkerheden til Styrelsen for Samfundssikkerhed. Underretningerne vil være fritaget for aktindsigt.

6.3 Finanstilsynet

Finanstilsynet forventer at blive orienteret om væsentlige it-hændelser – herunder hændelser, der berører personoplysninger – hos finansielle virksomheder og fælles datacentraler, idet indberetning af IKT-hændelser (informations- og kommunikationsteknologi-hændelser) er harmoniseret og strømlinet med DORA-forordningens ordning for indberetninger.

6.4 NIS2

NIS2 er den almindelige betegnelse for EU-direktiv (EU) 2022/2555, som fastlægger foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i EU. NIS2-direktivet bygger ovenpå og ophæver EU-direktivet om sikkerhed i net- og informationssystemer (NIS1-direktivet).

Formålet med NIS2-direktivet er at yderligere styrke og ensarte cybersikkerheden og modstandsdygtigheden overfor cybertrusler på tværs af EU for virksomheder inden for en lang række sektorer og for offentlige myndigheder, som anses for at være kritiske for økonomien og samfundet.

For de myndigheder og virksomheder, der er omfattet af NIS2, gælder der en forpligtelse til at indberette "væsentlige hændelser" til den relevante sektorspecifikke myndighed, der skal modtage og behandle indberetningerne.

Væsentlige hændelser kendetegnes ved, at de har:

1. Forårsaget eller er i stand til at forårsage alvorlige driftsforstyrrelser af tjenesterne eller økonomiske tab for den berørte enhed, eller
2. påvirket eller er i stand til at påvirke andre fysiske eller juridiske personer ved at forårsage betydelig materiel eller immateriel skade.

[14] Lovbekendtgørelse nr. 128 af 7. februar 2014 som senest ændret ved lovbekendtgørelse 955 af 17. juni 2022.

Man skal være opmærksom på, at der gælder tidsfrister for indberetning af "væsentlige hændelser" ifølge NIS2, som i nogle tilfælde er 24 timer. Denne tidsfrist har dog som udgangspunkt ikke betydning for den tidsfrist for anmeldelse af brud på persondatasikkerheden til Datatilsynet, der følger af databeskyttelsesforordningen, men det kan bl.a. af praktiske årsager – herunder ved brug af anmeldelsesblanketten på virk.dk – være hensigtsmæssigt at foretage anmeldelse samtidig.

7. Implementering i organisationen

For at kunne sikre en effektiv efterlevelse af forpligtelsen til at anmelde brud på persondatasikkerheden til Datatilsynet og til at underrette de registrerede, er det helt afgørende, at den dataansvarlige (og databehandlere) udarbejder procedurer for håndtering af sikkerhedshændelser i organisationen.

Den dataansvarlige bør i den sammenhæng indtænke forholdet til eventuelle databehandlere og underdatabehandlere således, at procedurerne også tager højde for brud på persondatasikkerheden hos databehandleren og eventuelle underdatabehandlere.

Ifølge Digitaliseringsstyrelsens guide til implementering af ISO-standarden (ISO27001) vil etableringen af en konkret proces for håndtering af sikkerhedshændelser f.eks. kunne indeholde følgende elementer:

- Rapportering og vurdering af hændelsen
- Ansvarsfordeling
- Håndtering
- Evaluering
- Forbedring

Den dataansvarlige (og databehandlere) bør endvidere overveje, hvilke tekniske og organisatoriske foranstaltninger der kan indføres i organisationen for at sikre, at et brud på persondatasikkerheden bliver opdaget, hvilket indebærer, at den dataansvarlige skal etablere passende procedurer og retningslinjer, som skal sikre, at brud bliver opdaget og behandlet korrekt. Den dataansvarlige skal i den forbindelse sikre sig, at alle medarbejdere i organisationen i nødvendigt omfang er bekendt med interne procedurer for håndtering af brud på persondatasikkerheden, og at relevante medarbejdere kan identificere, håndtere og vurdere brud på persondatasikkerheden.

En procesbeskrivelse af, hvordan en sikkerhedshændelse, herunder et brud på persondatasikkerheden, skal håndteres i organisationen bør bl.a. adressere, hvad der skal til før:

1. Den dataansvarlige/databehandleren kan foretage den fornødne rapportering om bruddet internt i organisationen, herunder beskrive fordelingen af ansvar for håndteringen af bruddet.
2. Den dataansvarlige/databehandleren kan stoppe bruddet.
3. Den dataansvarlige kan foretage den fornødne risikovurdering af bruddet.
4. Den dataansvarlige kan opfylde betingelsen om, at underrette Datatilsynet og de registrerede uden unødig forsinkelse (for anmeldelse til Datatilsynet – senest efter 72 timer).
5. Den dataansvarlige kan foretage den fornødne dokumentation af brud på persondatasikkerheden.

8. Opsummering

- Den dataansvarlige skal i tilfælde af et brud på persondatasikkerheden **uden unødig forsinkelse og om muligt inden 72 timer** foretage anmeldelse af bruddet til Datatilsynet via Virk.dk, **medmindre det er usandsynligt, at bruddet medfører en risiko for personers rettigheder eller frihedsrettigheder**.
- Den dataansvarlige skal være opmærksom på, om der gælder en anmeldelsespligt til en anden relevant myndighed.
- **Databehandleren** skal underrette den dataansvarlige om et brud **uden unødig forsinkelse**.
- Der er en række **minimumskrav til indholdet af anmeldelsen** (udfyldelse af blanket):
    - Karakteren af bruddet på persondatasikkerheden mv.
    - Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
    - De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
    - 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.
- **Anmeldelse** til Datatilsynet **kan ske trinvist.**
- Den dataansvarlige skal dokumentere **alle** brud, herunder de faktiske omstændigheder, konsekvenser og trufne afhjælpende foranstaltninger.

****

- Den dataansvarlige skal **underrette den registrerede, når** et brud på persondatasikkerheden sandsynligvis vil indebære en **høj risiko for fysiske personers rettigheder og frihedsrettigheder.**
- Den dataansvarlige skal underrette den enkelte registrerede **uden unødig forsinkelse**.
- Underretningen, der skal gives i et **klart og forståeligt sprog**, skal beskrive karakteren af bruddet og **mindst indeholde oplysninger om:**
    - Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
    - De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
    - 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.
- Det er **ikke nødvendigt at underrette den registrerede, hvis en af følgende betingelser er opfyldt:**
    1) Den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger.
    2) Den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registrerede ikke længere er reel.
    3) Det vil kræve en uforholdsmæssig indsats – i så fald skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.
    4) Der kan gøres undtagelse til underretningsforpligtelsen jf. national lovgivning

- Datatilsynet kan kræve, at der sker underretning af de registrerede.

- Der kan findes eksempler på brud, hvor der skal ske/ikke skal ske anmeldelse til Datatilsynet og/eller underretning af registrerede i EDPBs retningslinjer 01/2021 om eksempler på brud på persondatasikkerheden og EDPBs retningslinjer om anmeldelse af brud på persondatasikkerheden i henhold til GDPR. Begge retningslinjer kan findes på EDPBs hjemmeside og/eller på Datatilsynets hjemmeside, hvor du også finder denne vejledning.

- Er man som dataansvarlig i tvivl om, hvordan et brud skal håndteres – herunder om der skal ske anmeldelse af bruddet til Datatilsynet og/eller underretning af de registrerede – er man altid velkommen til at kontakte Datatilsynet (telefonisk) for at få råd og vejledning. Datatilsynet kan som udgangspunkt kontaktes telefonisk inden for telefonrådgivningens åbningstider, som kan findes på tilsynets hjemmeside.

Håndtering af brud på persondatasikkerheden
© 2025

Eftertryk med kildeangivelse er tilladt

Udgivet af:
Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Foto: Stock

ISBN: 978-87-999222-5-3

Datatilsynet
Carl Jacobsens Vej 35
2500 Valby
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk