DATATILSYNET

JUSTITSMINISTERIET

Vejledning om håndtering af brud på person-datasikkerheden

Januar 2018

Indhold

1.0 Forord

Med databeskyttelsesforordningen indføres der en generel forpligtelse for dataansvarlige til at anmelde brud på persondatasikkerheden til databeskyttelsesmyndigheden (Datatilsynet).

Dette er en ny forpligtelse, idet der ikke efter den nugældende persondatalov er pligt til at anmelde et sikkerhedsbrud til Datatilsynet. Derimod har der siden 2011 eksisteret en lovgivningsmæssig pligt for telesektoren og virksomheder, der er omfattet af den særlige telelovgivning, til at anmelde brud på persondatasikkerheden til Erhvervsstyrelsen. Herudover har der siden april 2017, som følge af den nye lov om retshåndhævende myndigheders behandling af personoplysninger (retshåndhævelsesloven), eksisteret en pligt for de retshåndhævende myndigheder til at anmelde brud på persondatasikkerheden til Datatilsynet.

Med databeskyttelsesforordningen indføres tillige en generel pligt for de dataansvarlige til at underrette de registrerede om et brud på persondatasikkerheden.

En sådan generel forpligtelse til at underrette de berørte personer i tilfælde af et sikkerhedsbrud er ligeledes ny, idet persondataloven ikke indeholder en specifik bestemmelse om underretning af den registrerede i forbindelse med et brud på persondatasikkerheden. Det følger dog i dag af Datatilsynets praksis, at den dataansvarlige i tilfælde, hvor personoplysninger er kommet til uvedkommendes kendskab eller har været i risiko herfor som følge af et brud på persondatasikkerheden som udgangspunkt skal underrette de berørte personer. En tilsvarende pligt til at underrette de registrerede gælder ligeledes efter den nye retshåndhævelseslov.

Da databeskyttelsesforordningens regler om anmeldelse og underretning af brud på persondatasikkerheden indeholder nogle meget korte tidsfrister, såvel som den dataansvarlige indenfor tidsfristen skal være i stand til at danne sig det fornødne overblik over sikkerhedsbruddet, er det vigtigt, at den dataansvarlige virksomhed eller myndighed (samt databehandlere) udarbejder faste procedurer for håndtering af sikkerhedsbrud. Disse procedurer skal samtidig være medvirkende til at den dataansvarlige hurtigst muligt kan tage hånd om sikkerhedsbruddet, herunder sikre at der ikke sker yderligere kompromittering af personoplysninger som følge af bruddet.

Det skal i tilknytning hertil nævnes, at den dataansvarliges (og databehandlerens) manglende efterlevelse af reglerne om anmeldelse og underretning kan resultere i, at disse bliver idømt en bødestraf i henhold til databeskyttelsesforordningens artikel 83.

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/eller pligt til at underrette de berørte personer.

Herudover indeholder vejledningen en gennemgang af de indholdsmæssige krav til en anmeldelse/underretning om et sikkerhedsbrud, ligesom der i vejledningen vil blive redegjort for forordningens krav til tidspunktet for, hvornår der skal ske anmeldelse/underretning, samt måden hvorpå anmeldelsen skal indgives til Datatilsynet.

Som bilag A til vejledningen finder du et flowchart, som illustrerer de relevante skridt for den dataansvarlige i forbindelse med et brud på persondatasikkerheden. Du finder endvidere som bilag B en oversigt over de enkelte krav til en anmeldelse / underretning, ligesom du i bilag C kan se en række eksempler på brud på persondatasikkerheden, og hvem der i så fald skal underrettes. Herudover finder du i bilag D og E et eksempel på henholdsvis en blanket til brug for anmeldelse til Datatilsynet og en blanket til brug for underretning af de registrerede.
Ønsker du en nærmere gennemgang af reglerne om anmeldelse og underretning af brud på persondatasikkerheden, kan du bl.a. læse afsnittene 5.11. og 5.12. i betænkning nr. 1565/2017 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning.

Du kan også læse Artikel 29-gruppens vejledning i WP 250 af 3. oktober 2017 om “Guidelines on Personal data breach notification under Regulation 2016/679”. Vejledningen kan findes her.

2.0 Hvad er et brud på persondatasikkerheden?

2.1 Definition

Efter databeskyttelsesforordningens artikel 4, nr. 12 er et brud på persondatasikkerheden:

"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."

Det er således alene de *sikkerhedshændelser*, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til **personoplysninger**, der er omfattet af databeskyttelsesforordningens definition af et brud på persondatasikkerheden.

Der gøres i den forbindelse være opmærksom på, at en sikkerhedshændelse ikke altid vil være et brud på persondatasikkerheden, hvorimod det omvendte altid vil være tilfældet. Som et eksempel herpå kan nævnes flere forgæves forsøg på log-in, som vil være at betragte som en sikkerhedshændelse, uden at der samtidig er tale om et brud på persondatasikkerheden.

Personoplysninger er enhver form for information, der kan henføres til bestemte personer, også selv om dette forudsætter kendskab til et personnummer, registreringsnummer eller lignende. Også oplysninger i form af f.eks. et billede eller et fingeraftryk er personoplysninger.

Selv om oplysninger som et navn eller en adresse er erstattet af en kode, er det stadig en personoplysning, hvis koden kan føres tilbage til den oprindelige personoplysning. F.eks. er oplysninger, der er krypteret, fortsat personoplysninger, så længe der er nogen, der kan gøre oplysningerne læsbare og identificere de personer, det drejer sig om.

En **behandling** omfatter enhver form for håndtering af personoplysninger. Det kan f.eks. være indsamling, registrering, systematisering, opbevaring, søgning, brug, videregivelse eller sletning af oplysninger.

Bliver det i forbindelse med en sikkerhedshændelse konstateret, at der er sket et brud på persondatasikkerheden, skal den dataansvarlige vurdere, om der er pligt til at underrette Datatilsynet og de berørte personer om bruddet.

2.2 Typer af brud på persondatasikkerheden – hvornår går det galt?

Et sikkerhedsbrud kan inddeles i tre forskellige kategorier:

- **Brud på fortroligheden -** Dvs. brud, der indebærer uautoriseret eller utilsigtet videregivelse af eller adgang til personoplysninger.

Eksempel: En kommune har ved en fejl offentliggjort fortrolige oplysninger om kommunens borgere på sin hjemmeside.

- **Brud på tilgængeligheden –** Dvs. brud, der indebærer manglende adgang til eller tilintetgørelse af personoplysninger.

Eksempel: En tandlægeklinik bliver udsat for ransomware, idet kriminelle personer har tiltvunget sig adgang til klinikkens it-systemer og bl.a. forhindret klinikkens medarbejdere i at få adgang til de elektroniske klientjournaler. Der forlanges nu en løsesum for at "tilbagelevere" oplysningerne til tandlægeklinikken.

Der kan også være tale om brud på tilgængeligheden i tilfælde af, at en virksomhed eller myndighed oplever en midlertidig afbrydelse af den normale drift, f.eks. som følge af en strømafbrydelse.

- **Brud på integriteten –** Dvs. brud, der indebærer hændelig eller ulovlig ændring af personoplysninger.

Eksempel: Et forsikringsselskab opdager, at der som følge af en systemfejl er sket ændringer i de oplysninger, som er registreret i selskabets kundedatabase.

Det skal bemærkes, at et sikkerhedsbrud sagtens kan omfatte flere af de ovennævnte typer af brud på persondatasikkerheden.

Et brud på persondatasikkerheden er ofte begrundet i utilstrækkelig sikkerhed hos den dataansvarlige, der typisk vil høre under en eller flere af de nedenstående kategorier:

- **Systemmæssige fejl –** F.eks. it-systemer, der ikke er indrettet i overensstemmelse med de persondataretlige krav.

Eksempel: En kommune har ikke sikret sig den fornødne adgangsbegrænsning på kommunens it-systemer, hvilket medfører, at flere af kommunens medarbejdere har adgang til oplysninger om kommunens borgere, som de ikke har et arbejdsmæssigt behov for at have adgang til.

- **Organisatoriske fejl** – F.eks. manglende undervisning eller instruktion af medarbejdere eller manglende fastsættelse af interne retningslinjer for it-sikkerhed.

Eksempel: En privat virksomhed benytter en ekstern it-leverandør til hosting af virksomhedens kundedata. Virksomheden har dog ikke foretaget en forudgående kontrol af leverandørens it-sikkerhed. Leverandøren bliver ramt af et virusangreb, der også påvirker virksomhedens kundedata. Det viser sig, at angrebet kunne have været undgået, hvis leverandøren havde installeret bedre firewalls på sine it-systemer.

- **Menneskelige fejl** – F.eks. utilsigtet videregivelse af personoplysninger til en forkert modtager.

Eksempel: En medarbejder, som er ansat hos en offentlig myndighed, benytter en ukrypteret e-mail til at fremsende dokumenter, der indeholder fortrolige personoplysninger, herunder oplysninger om en persons cpr-nummer.

2.3 Hvad er de mulige konsekvenser af et brud på persondatasikkerheden?

Et brud på persondatasikkerheden kan ende med at få betydelige konsekvenser for de berørte personer, hvis ikke der tages tilstrækkeligt og rettidigt hånd om bruddet.

Databeskyttelsesforordningen beskriver bl.a., at et brud på persondatasikkerheden kan påføre fysiske personer fysisk, materiel eller immateriel skade, såsom tab af kontrol over deres personoplysninger eller begrænsning af deres rettigheder, forskelsbehandling, identitetstyveri eller -svig, finansielle tab, uautoriseret ophævelse af pseudonymisering, skade på omdømme, tab af fortrolighed for oplysninger, der er omfattet af tavshedspligt, eller andre betydelige økonomiske eller sociale konsekvenser.

Den dataansvarlige bør derfor, så snart denne bliver bekendt med, at der er sket et brud på persondatasikkerheden, anmelde bruddet til den kompetente tilsynsmyndighed uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet.

Det vil dog ikke være nødvendigt, at anmelde et brud på persondatasikkerheden til Datatilsynet, hvis den dataansvarlige kan påvise, at bruddet sandsynligvis ikke indebærer risiko for fysiske personers rettigheder eller frihedsrettigheder.

Hvilke typer af brud på persondatasikkerheden, der kræver anmeldelse til Datatilsynet og/eller underretning af de berørte personer, samt hvilke krav der stilles til anmeldelsen/underretningen vil blive nærmere beskrevet nedenfor.

3.0 Anmeldelse af brud på persondatasikkerheden til Datatilsynet

3.1 Hvilke brud på persondatasikkerheden kræver anmeldelse?

Det følger af databeskyttelsesforordningens artikel 33, stk. 1, at

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

Det er således først og fremmest en forudsætning for, at der skal ske anmeldelse til Datatilsynet, at der er sket et brud på persondatasikkerheden. Læs mere om, hvornår der er tale om et brud på persondatasikkerheden ovenfor under afsnit 2.1.

Det er dernæst en forudsætning, at det ikke er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

3.1.1 Risiko for fysiske personers rettigheder eller frihedsrettigheder

Med *fysiske personers rettigheder eller frihedsrettigheder* tænkes især på retten til beskyttelse af personoplysninger, som følger af Den Europæiske Unions Charter om Grundlæggende Rettigheder (artikel 8).

De øvrige rettigheder og frihedsrettigheder, der følger af chartret, kan dog også være relevante at tage i betragtning i forbindelse med et brud på persondatasikkerheden. Det kan f.eks. vurderes, at et brud på persondatasikkerheden kan få konsekvenser for de berørte personers ret til privatliv (chartrets artikel 7).

3.1.2 Vurdering af risikoen

For den dataansvarlige vil en vurdering af bruddets omfang og sandsynlige risiko for de berørte personer ikke alene være nødvendig for at kunne håndtere og afhjælpe et brud på persondatasikkerheden, men også for at kunne afgøre, om der skal ske anmeldelse til Datatilsynet.

Til forskel for en vurdering af den potentielle risiko, som den dataansvarlige f.eks. skal foretage i forbindelse med en konsekvensanalyse (DPIA), vil en risikovurdering efter databeskyttelsesforordningens artikel 33 og 34 tage sit udgangspunkt i den allerede indtrufne risiko for de berørte personer som følge af et brud på persondatasikkerheden.

Ifølge databeskyttelsesforordningen skal den dataansvarlige, når denne vurderer risikoen ved et brud på persondatasikkerheden, både undersøge risikoens **sandsynlighed** og **alvor** for de berørte personers rettigheder og frihedsrettigheder.

Artikel 29-gruppen anbefaler i den forbindelse, at følgende kriterier tages i betragtning, når der skal foretages en vurdering af risikoen for de registreredes rettigheder og frihedsrettigheder som følge af et brud på persondatasikkerheden:

- **Typen af brud**

Hvilke konsekvenser 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 få andre konsekvenser for den registrerede, end hvis der f.eks. er tale om et brud, der resulterer i offentliggørelse af personoplysninger.

- **Karakteren, følsomheden og omfanget af de personlige oplysninger**

Som udgangspunkt vil *typen af personoplysninger* have indflydelse på risikovurderingen. Desto mere følsomme personoplysninger, der er tale om, desto større konsekvenser må et sikkerhedsbrud formodes at få for de berørte personer. En utilsigtet offentliggørelse af oplysninger om, at en person har begået strafbare forhold, har opbygget en stor gæld eller lider af en bestemt sygdom må f.eks. formodes at kunne få mere vidtrækkende konsekvenser for den pågældende, end hvis f.eks. den pågældendes e-mailadresse eller cv bliver offentliggjort.

Det er dog i den forbindelse vigtigt at holde sig for øje, at alle omstændigheder omkring et utilsigtet læk af personoplysninger tages i betragtning, herunder hvis der er særlige hensyn, der gør sig gældende for de personer, hvis oplysninger er blevet eksponeret. Offentliggørelse af adresseoplysninger vil normalt ikke forventes at kunne få alvorlige konsekvenser, hvorimod dette kan forholde sig anderledes, hvis adressen afslører, at den pågældende er bosiddende på et bosted for personer i misbrugsbehandling.

Omfanget af bruddet, herunder *mængden* af personoplysninger, der er berørt, vil ligeledes kunne få betydning for udfaldet af risikovurderingen. På den ene side vil kompromittering af en lille mængde meget følsom persondata kunne forårsage stor skade, mens det på den anden side kan få tilsvarende store konsekvenser, hvis en større mængde lækkede oplysninger tilsammen afslører informationer til skade for den/de berørte. Som et eksempel herpå kan nævnes, hvis en bank via e-mail ved en fejl videregiver oplysninger om en kundes personnummer og adgangskode til kundens netbank, idet oplysningerne i sin sammenhæng vil kunne misbruges til at opnå adgang til oplysninger om kundens låneforhold, gæld mv.

Den tidsmæssige udstrækning af et brud vil også kunne få betydning, da det alt andet lige må forudsættes, at risikoen for de registrerede er større, hvor oplysningerne har været tilgængelige for uvedkommende i en længere periode. Det er dog ikke udelukket, at selv et kortvarigt brud kan få store konsekvenser, f.eks. hvor en myndighed opdager, at der i få timer har været adgang til deres it-systemer, og samtidig konstaterer, at der har været ukendte personer inde i systemerne.

- **Muligheden for at identificere personer**

En faktor, som ligeledes kan spille ind ved risikovurderingen er spørgsmålet om, hvor nemt det vil være at foretage en identifikation af personen ud fra de oplysninger, som er blevet kompromitteret, eller at matche oplysningerne med anden information, som vil kunne identificere den pågældende.

I den sammenhæng vil det kunne få betydning, hvis den dataansvarlige har beskyttet oplysningerne ved f.eks. at anvende kryptering eller pseudonymisering, da det som følge heraf ikke umiddelbart vil være muligt at identificere vedkommende.

- **Alvorligheden af konsekvenserne for de berørte personer**

Det er tidligere under afsnit 2.3. omtalt, hvilke mulige konsekvenser et brud på persondatasikkerheden kan medføre.

Artikel 29-gruppen nævner i den sammenhæng, at et brud, der forårsager kompromittering af oplysninger om særligt sårbare eller udsatte personer vil kunne vurderes at have større skadevirkning. Det samme vil formentlig være tilfældet, hvis der er tale om oplysninger om børn.

Hvis det er den dataansvarlige bevidst, at de involverede personoplysninger er endt i hænderne på kriminelle personer, som forventes at have onde hensigter med deres kendskab til oplysningerne, vil dette kunne have stor betydning for risikovurderingen. Hvis oplysningerne omvendt er endt hos en forkert modtager, som den dataansvarlige har stor tillid til, og forventer vil tilbagelevere eller destruere oplysningerne efter instruks fra den dataansvarlige, vil dette kunne føre til, at den dataansvarlige vurderer, at der ikke er konsekvenser forbundet med videregivelsen, og at der derfor ikke skal anmeldelse til Datatilsynet. Den dataansvarlige bør dog være yderst sikker i sin sag, når modtagerens troværdighed tillægges betydning for denne vurdering. Den dataansvarlige bør samtidig – hvis muligt – sikre sig dokumentation for, at vedkommende ikke længere har rådighed over oplysningerne.

Endelig vil konsekvenserne ved et sikkerhedsbrud som udgangspunkt være større, hvis de er af længerevarende og mere permanent karakter og ikke uden videre kan afhjælpes af den dataansvarlige eller af den registrerede selv. Hvis f.eks. der sker et læk af en persons dankortoplysninger vil de mulige konsekvenser heraf relativt nemt kunne reduceres ved at spærre betalingskortet. Hvis der omvendt sker læk af oplysninger, som kan skade en persons ære eller omdømme, vil dette kunne få mere vidtrækkende konsekvenser for vedkommende.

- **Særlige karaktertræk ved den registrerede**

Som nævnt ovenfor kan det få betydning for risikovurderingen, hvis der er tale om oplysninger vedrørende et barn eller anden sårbar person. Der kan dog også foreligge andre omstændigheder ved vedkommende, som kan få indflydelse på de konsekvenser, som den pågældende kan blive mødt af som følge af et sikkerhedsbrud. Dette kunne være tilfældet, hvis der f.eks. sker offentliggørelse af adresse- eller kontaktoplysninger på en person, som er offentligt kendt eller under vidnebeskyttelse.

- **Antallet af berørte personer**

Som udgangspunkt vil betydningen af et brud på persondatasikkerheden stige i takt med antallet af personer, som er berørt heraf. Det er dog bestemt ikke udelukket, at kompromittering af oplysninger om en enkelt eller få personer også vil kunne få alvorlige konsekvenser.

- **Særlige karaktertræk ved den dataansvarlige**

Hvilken type af dataansvarlig myndighed eller virksomhed, der er tale om, samt hvilke behandlingsaktiviteter denne foretager sig, kan påvirke sandsynligheden for, at et sikkerhedsbrud hos den dataansvarlige vil indebære en risiko for de berørte personer. Hvis der f.eks. er tale om et privathospital, der behandler et stort omfang af helbredsoplysninger, eller et kreditoplysningsbureau, der behandler oplysninger om folk, der er registreret som dårlige betalere, vil et brud på persondatasikkerheden, på grund af den dataansvarliges særlige karakter, være forbundet med en større risiko for de registrerede.

3.1.3 Opsummering

Det må lægges til grund, at jo mere *alvorlige* konsekvenser bruddet kan medføre, jo større vil risikoen være for de berørte personer. Tilsvarende vil en større *sandsynlighed* for, at et brud vil få konsekvenser for de registrerede ligeledes indebære en større risiko.

Når den dataansvarlige har taget ovenstående faktorer omkring bruddet i betragtning, skal den dataansvarlige herefter vurdere, om der er grundlag for at foretage anmeldelse til Datatilsynet.

Hvis den dataansvarlige er i tvivl, bør den dataansvarlige for en sikkerheds skyld anmelde bruddet til Datatilsynet.

3.2 Situationer, hvor anmeldelse til Datatilsynet ikke er nødvendig

Det følger af databeskyttelsesforordningen, at et brud på persondatasikkerheden ikke skal anmeldes til tilsynsmyndigheden, hvis det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Der må imidlertid være en rimelig høj grad af sikkerhed herfor.

At et brud på persondatasikkerheden vurderes 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 evne til at konstatere, om personoplysninger er kommet til uvedkommendes kendskab.

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, påhviler den dataansvarlige.

Eksempel 1: Personalechefen i en virksomhed får på togturen hjem fra arbejde stjålet sin taske, hvori der bl.a. ligger en ekstern harddisk indeholdende oplysninger om ansøgere til en opslået stilling i virksomheden. Virksomheden har sikret sig, at de harddiske, der udleveres til medarbejderne, er beskyttet med en stærk kryptering, der ikke umiddelbart vil være mulig for uvedkommende at dekryptere.

I det ovennævnte eksempel kan der, på baggrund af den beskyttelse af de indeholdte oplysninger, som krypteringen af harddisken sikrer, være skabt tilstrækkelig formodning om, at det er usandsynligt, at tabet af harddisken indebærer en risiko for de pågældende jobansøgere. Den dataansvarlige vil således kunne vurdere, at det pågældende brud på persondatasikkerheden ikke skal anmeldes til Datatilsynet. Den dataansvarlige vil dog stadig være forpligtet til at foretage intern dokumentation af bruddet. Læs mere om den dataansvarliges pligt til at foretage intern dokumentation under afsnit 3.6.

Den dataansvarlige skal dog i den forbindelse være opmærksom på, at risikobilledet kan ændre sig med tiden. I eksemplet med den mistede harddisk kan det efterfølgende vise sig, at den anvendte kryptering ikke er stærk nok, og at det derfor relativt nemt vil kunne lade sig gøre at bryde den. Det kan også vise sig, at uvedkommende kan være kommet i besiddelse af harddiskens krypteringsnøgle. Dette kan f.eks. være tilfældet, hvis virksomheden bliver udsat for et hackerangreb, hvor udefrakommende tiltvinger sig adgang til det it-system, hvor virksomheden opbevarer deres krypteringsnøgler.

Hvis risikobilledet ændrer sig således, at den dataansvarlige vurderer, at personoplysningerne ikke længere er tilstrækkeligt beskyttet, skal den dataansvarlige anmelde bruddet på persondatasikkerheden til Datatilsynet.

Som nævnt, kan det i forbindelse med et brud på persondatasikkerheden ligeledes blive konstateret, at den dataansvarlige har reageret så hurtigt, at bruddet ikke har medført kompromittering af personoplysninger.

Eksempel 2: En medarbejder hos en kommune kommer ved en fejl til at uploade en fil på kommunens hjemmeside, der indeholder personnumre på flere borgere i kommunen. Medarbejderen bliver straks opmærksom på fejlen og fjerner filen fra hjemmesiden. Kommunens it-afdeling kan ved en undersøgelse af hjemmesidens log-oplysninger konstatere, at der ikke har været besøgende på hjemmesiden i den tid, hvor filen har været tilgængelig. Kommunen konkluderer samtidig, at der ikke er noget der tyder på, at filen er blevet kopieret af søgemaskiner, som f.eks. Google, Bing og lign. På den baggrund vurderer kommunen, at sandsynligheden for at filen er eller kan komme til uvedkommendes kendskab er så lille, at der ikke skal ske anmeldelse til Datatilsynet.

Det kan ligeledes tænkes, at et brud på persondatasikkerheden, der har resulteret i sletning eller ændring af personoplysninger, ikke indebærer en risiko for de berørte personer, hvis den dataansvarlige har foretaget tilstrækkelig backup af sine systemer til at kunne gendanne oplysningerne uden konsekvenser for de registrerede.

I tilfælde af, at den dataansvarlige bliver ramt af en strømafbrydelse, der medfører at den dataansvarlige i en periode ikke kan få adgang til sit kundekartotek, vil heller ikke nødvendigvis kræve anmeldelse til Datatilsynet. Dette forudsætter dog, at den dataansvarlige vurderer, at den manglende adgang til personoplysninger ikke har konsekvenser for de pågældende kunder.

Det er dog vigtigt at understrege, at den dataansvarlige ved en vurdering af risikoen for de berørte personers rettigheder, som kan være forbundet med et brud på persondatasikkerheden, skal tage alle omstændighederne ved det pågældende brud i betragtning. Den dataansvarlige skal på den

ene side tage de sikkerhedsforanstaltninger, som kan reducere risikoen for de berørte personer i betragtning, og på den anden side de omstændigheder ved bruddet, der kan forhøje risikoen.

Det er således det samlede *aktuelle* risikobillede, der er afgørende for, om der skal ske anmeldelse af et brud på persondatasikkerheden til Datatilsynet.

3.3 Tidspunktet for anmeldelse

3.3.1 Hvad siger reglerne?

Hvis det er sandsynligt, at et brud på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder, skal den dataansvarlige anmelde bruddet til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer efter, at denne er blevet bekendt med bruddet.

Idet forordningen ikke omtaler dette, må det lægges til grund, at tidsfristen på de 72 timer løber uanset, om den dataansvarlige bliver bekendt med bruddet uden for normal kontortid, herunder i weekender og på helligdage.

Som det fremgår af bestemmelsens ordlyd, skal den dataansvarliges anmeldelse af et brud på persondatasikkerheden som hovedregel ske *uden unødig forsinkelse*. Heri ligger, at den dataansvarlige er forpligtet til at underrette Datatilsynet om bruddet, så snart det er muligt – også selvom dette tidspunkt indtræder, før udløbet af de 72 timer. Tidsgrænsen på de 72 timer skal med andre ord ikke forstås således, at den dataansvarlige kan vente med at anmelde et brud på persondatasikkerheden indtil fristen, hvis den dataansvarlige er i stand hertil på et tidligere tidspunkt.

Vedrørende spørgsmålet om, hvorvidt anmeldelse har fundet sted *uden unødig forsinkelse* beskriver databeskyttelsesforordningen endvidere, at dette bør fastslås 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 med risiko for yderligere kompromittering af personoplysninger, vil den dataansvarlige formentlig kunne retfærdiggøre en vis forsinkelse som følge af den dataansvarliges bestræbelser på at standse bruddet.

Tilsvarende må en vis forsinkelse kunne forsvares i tilfælde af, at den dataansvarlige er bekendt med, at personoplysninger er endt i hænderne på personer, der har til hensigt at benytte disse til kriminelle formål, og derfor i første omgang prioriterer at få forhindret dette, ved f.eks. at gå i dialog med politiet.

Det er imidlertid svært at forestille sig situationer, der gør det umuligt for den dataansvarlige at foretage anmeldelse til Datatilsynet inden for de 72 timer. Selv i den situation, hvor den dataansvarlige bliver ramt af et it-nedbrud, der forhindrer den dataansvarlige i at kunne foretage elektronisk underretning af Datatilsynet, vil den dataansvarlige i stedet kunne opfylde kravet om at anmeldelse skal ske uden unødig forsinkelse, ved at indrapportere bruddet telefonisk eller via postvæsnet, f.eks. ved at benytte et såkaldt quickbrev.

Tidsgrænsen på de 72 timer for anmeldelse til Datatilsynet er dog ikke definitiv. Men indgives anmeldelsen efter udløbet af fristen på de 72 timer, skal anmeldelsen ledsages af en begrundelse for forsinkelsen. Overskrides de 72 timer, skal den dataansvarlige således være i stand til at redegøre for de særlige grunde, der umuliggjorde anmeldelse til Datatilsynet inden for fristen. Der henvises i øvrigt til afsnit 3.5.3. nedenfor.

Der gøres i den forbindelse endvidere opmærksom på muligheden for at foretage trinvis anmeldelse til Datatilsynet, som vil blive nærmere beskrevet under afsnit 3.5.2.

3.3.2 Hvordan skal det ske i Danmark?

Databeskyttelsesforordningen er ikke den eneste lovgivning i Danmark, der indebærer en pligt til – under visse omstændigheder – at anmelde en it-sikkerhedshændelse til rette myndighed. Som eksempel vil visse forsyningsvirksomheder og andre operatører af væsentlige tjenester samt udbydere af digitale tjenester skulle underrette de nationale myndigheder I tilfælde af væsentlige sikkerhedshændelser i medfør af det såkaldte NIS-direktiv. Et andet eksempel herpå er offentlige myndigheders forpligtelse til at indberette større it-sikkerhedsmæssige hændelser i deres digitale infrastruktur til Center for Cybersikkerhed.

En it-sikkerhedshændelse kan være omfattet af flere af de lovpligtige indberetningsordninger, og for at gøre det nemt og enkelt for virksomheder og myndigheder at indberette sikkerhedshændelser på tværs af de relevante myndigheder, der skal underrettes, bliver der etableret én fælles digital løsning for indberetning af sikkerhedshændelser via hjemmesiden virk.dk.
Såfremt et it-sikkerhedsbrud indebærer kompromittering af personoplysninger, vil den dataansvarlige således kunne angive Datatilsynet som modtager af den pågældende indberetning.

Der gøres i øvrigt opmærksom på, at den dataansvarlige i forbindelse med en anmeldelse af et brud på persondatasikkerheden til Datatilsynet via den digitale indberetningsløsning, har mulighed for at tilkendegive, om den dataansvarlige samtidig ønsker at politianmelde bruddet. Dette kunne f.eks. være tilfældet, hvis den dataansvarlige har været udsat for et hackerangreb.
Den digitale indberetningsløsning vil være tilgængelig, når databeskyttelsesforordningen får virkning den 25. maj 2018. Det vil til den tid være muligt at finde et link til den digitale indberetningsløsning via datatilsynets hjemmeside: www.datatilsynet.dk

Indberetningsløsningen vil i første omgang bestå af en elektronisk blanketløsning med tekstfelter, som skal udfyldes af den dataansvarlige. Nogle af tekstfelterne vil give mulighed for at tilføje fritekst, hvor andre af felterne består af såkaldte ”checkboxes”, hvor den dataansvarlige skal sætte kryds ud for ét eller flere af de i blanketten angivne valgmuligheder. Ved udformningen af blanketten er der taget hensyn til de minimumskrav til indholdet af en anmeldelse til Datatilsynet, som vil blive nærmere beskrevet nedenfor under afsnit 3.5.

3.3.2.1. Hvem kan foretage anmeldelse til Datatilsynet?

Som udgangspunkt er det alene den dataansvarlige, som kan 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 bruddet 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, f.eks. ved fuldmagt, og at adgangen hertil fremgår af den databehandleraftale, der er indgået mellem parterne.

Det er dog vigtigt i den forbindelse at understrege, at det overordnede juridiske ansvar for at anmelde et brud på persondatasikkerheden, herunder at dette sker rettidigt, forbliver hos den dataansvarlige uanset, at den dataansvarlige har bemyndiget databehandleren til at anmelde bruddet til Datatilsynet.

3.3.3 Hvornår bliver den dataansvarlige "bekendt" med bruddet?

Som det endvidere fremgår af bestemmelsens ordlyd, aktiveres den dataansvarliges forpligtelse til at foretage anmeldelse til Datatilsynet, efter at den dataansvarlige er *blevet bekendt med, at der er sket et brud på persondatasikkerheden*. En simpel formodning om, at et brud på persondatasikkerheden har fundet sted, eller en simpel påvisning af en hændelse vil i den forbindelse ikke være tilstrækkeligt til at anse et brud på persondatasikkerheden for at være "sket". En sådan simpel formodning bør dog føre til, at den dataansvarlige undersøger sagen nærmere med henblik på at afklare, om der rent faktisk er sket et brud på persondatasikkerheden.

I vurderingen af, om der er "sket" et brud på persondatasikkerheden må det antages, at der kan lægges vægt på, om de oplysninger, som den dataansvarlige efter bestemmelsen er forpligtet til at meddele Datatilsynet i forbindelse med et brud, står til rådighed for den dataansvarlige. Læs mere om, hvilke oplysninger, der skal meddeles Datatilsynet, under afsnit 3.5.
Der kan i den forbindelse også henvises til den EU forordning, der regulerer, hvilke foranstaltninger udbydere af offentligt tilgængelige kommunikationstjenester skal anvende ved underretning om brud på persondatasikkerheden, hvoraf det bl.a. fremgår, *at et brud på persondatasikkerheden skal anses for at være påvist, hvis en udbyder har opnået tilstrækkelig kendskab til, at en sikkerhedshændelse er indtruffet, og at den har kompromitteret persondatasikkerheden, således at der kan afgives en hensigtsmæssig underretning som krævet ifølge denne forordning.*
En tilsvarende tilgang må kunne anvendes ved et brud på persondatasikkerheden hos en dataansvarlig, som er omfattet af databeskyttelsesforordningen.

3.4 Hvilke forpligtelser har databehandleren?

Det følger af databeskyttelsesforordningens artikel 33, stk. 2, at

"Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket et brud på persondatasikkerheden."

En databehandler, er typisk en virksomhed, offentlig myndighed eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne og efter instruks fra den dataansvarlige.

Databehandleren skal under alle omstændigheder underrette den dataansvarlige om et brud på persondatasikkerheden – også selvom databehandleren er af den opfattelse, at bruddet ikke indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder. Databehandleren bør i øvrigt underrette den dataansvarlige uanset, at databehandleren har en formodning om, at den dataansvarlige allerede er bekendt med bruddet.

Bestemmelsen indeholder ikke en udtrykkelig tidsfrist for, hvornår databehandleren, efter at være blevet opmærksom på et brud på persondatasikkerheden, skal underrette den dataansvarlige. Det fremgår dog af bestemmelsen, at databehandleren skal underrette den dataansvarlige *uden unødig forsinkelse.*

Artikel 29-gruppen anbefaler i den forbindelse, at databehandleren *straks* underretter den dataansvarlige og herefter følger op med den eventuelle 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.

Ifølge databeskyttelsesforordningens artikel 28, stk. 3, skal databehandleraftalen mellem den dataansvarlige bl.a. forpligte databehandleren til at bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i artikel 33 om anmeldelse af brud på persondatasikkerheden til Datatilsynet, under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren jf. artikel 28, stk. 3, litra f.
Databehandleraftalen bør endvidere indeholde en udtrykkelig forpligtelse for databehandleren til straks at underrette den dataansvarlige i tilfælde af et brud på persondatasikkerheden.

3.4.1 Underdatabehandlere

Hvis en databehandler gør brug af en anden databehandler (underdatabehandler), er underdatabehandleren underlagt de samme databeskyttelsesforpligtelser som dem, der er fastsat i databehandleraftalen mellem den dataansvarlige og den primære databehandler. Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver den primære databehandler fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser. Dette følger af databeskyttelsesforordningens artikel 28. stk. 4.

Underdatabehandleren er derfor på lige fod med den primære databehandler forpligtet til at bistå den dataansvarlige i tilfælde af et brud på persondatasikkerheden, dog under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for underdatabehandleren.

Hvis den dataansvarlige vurderer, at det er forsvarligt under hensyn til overholdelsen af den dataansvarliges forpligtelser i henhold til artikel 33, kan den dataansvarlige vælge, at delegere ansvaret for at underrette den dataansvarlige samt at forestå den videre dialog mellem den dataansvarlige og underdatabehandleren til den primære databehandler.

Eftersom, at det er den primære databehandler, der er ansvarlig for underdatabehandlerens forpligtelser over for den dataansvarlige, bør den primære databehandler sikre sig at kunne leve op til sine egne forpligtelser efter artikel 33, stk. 2, ved i kontrakten mellem den primære databehandler og underdatabehandleren, at forpligte underdatabehandleren til straks at underrette den primære databehandler om et eventuelt brud på persondatasikkerheden.

Afhængigt af om der i aftalen mellem den primære databehandler og den dataansvarlige er indsat en tilsvarende forpligtelse, kan underdatabehandleren således være forpligtet til både at skulle underrette den dataansvarlige og den primære databehandler i anledning af en sikkerhedsbrist.

3.5 Hvilke oplysninger skal meddeles?

3.5.1 Hvad siger reglerne?

> Det følger af databeskyttelsesforordningens artikel 33, stk. 3, litra a-d, at
> "Den i stk. 1 omhandlede anmeldelse skal *mindst*:
>
> a) beskrive karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
>
> b) angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes
>
> c) beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden
>
> d) beskrive de foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere bruddet på persondatasikkerheden, herunder, hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger."

Som det fremgår af bestemmelsen, angiver denne, hvilke oplysninger en anmeldelse til Datatilsynet *som minimum* skal indeholde. Bestemmelsen udelukker dermed ikke, at der skal/kan afgives yderligere informationer til Datatilsynet.

3.5.1.1. Ad litra a

Det fremgår af artikel 33, stk. 3, litra a, at anmeldelsen skal 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.

Som led i beskrivelsen af karakteren af bruddet skal den dataansvarlige oplyse, hvad der er sket. Det vil sige, at den dataansvarlige skal beskrive, på hvilken måde personoplysninger er blevet kompromitteret, f.eks. om der er sket utilsigtet offentliggørelse, tab eller ændring af personoplysninger. I tilknytning hertil skal den dataansvarlige præcisere, hvordan der er sket f.eks. tab af personoplysninger, hvilket bl.a. kan skyldes, at den dataansvarlige har været udsat for tyveri.

Som det fremgår af bestemmelsens ordlyd, skal den dataansvarlige oplyse det omtrentlige antal berørte personer samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger. Som følge heraf vil den dataansvarlige bl.a. skulle oplyse, hvis der er tale om følsomme personoplysninger, og i så fald, hvilken type af følsomme personoplysninger, der er tale om. Som det ligeledes fremgår af bestemmelsen vil den dataansvarlige kunne nøjes med at oplyse det

omtrentlige antal personer, der er berørt af bruddet samt det omtrentlige antal berørte registreringer. Med *registreringer* må menes, at den dataansvarlige, hvis der f.eks. er tale om utilsigtet offentliggørelse af cpr-numre, skal angive det omtrentlige antal af cpr-numre, som har været offentliggjort.

Endelig skal den dataansvarlige angive en "tidslinje" for det indtrufne brud på persondatasikkerheden, herunder ved oplysning om dato og tidspunkt for bruddets start og afslutning.

Henvis til bilag D (blanket til brug for anmeldelse til Datatilsynet).

3.5.1.2. Ad litra b

Af § 33, stk. 3, litra b, fremgår det, at anmeldelsen endvidere skal angive navn på og kontaktoplysninger for databeskyttelsesrådgiveren (DPO) eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.

Hvis Datatilsynet, efter at have modtaget en anmeldelse om et brud på persondatasikkerheden, ønsker yderligere oplysninger, vil Datatilsynet således tage kontakt til databeskyttelsesrådgiveren eller det eventuelle andet kontaktpunkt for at få oplysningerne fra den dataansvarlige.

3.5.1.3. Ad litra c

Herudover skal anmeldelsen ifølge artikel 33, stk. 3, litra c, beskrive de sandsynlige konsekvenser af bruddet på persondatasikkerheden.

Den dataansvarlige skal således angive de konsekvenser, som den dataansvarlige ved eller har en vis formodning om, at det bruddet kan forårsage. Der henvises i den forbindelse til afsnit 2.3. ovenfor.

3.5.1.4. Ad litra d

Det fremgår endelig af artikel 33, stk. 3, litra d, at anmeldelsen skal 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.

I beskrivelsen heraf skal den dataansvarlige bl.a. oplyse, om de berørte personer er blevet underrettet om bruddet på persondatasikkerheden i henhold til databeskyttelseslovens artikel 34.

På Datatilsynets hjemmeside nævnes en række tiltag, som kan være relevante for den dataansvarlige at foretage sig som led i håndteringen af en sikkerhedsbrist, der har ført til utilsigtet offentliggørelse eller videregivelse af personoplysninger:

Relevante skridt ved utilsigtet offentliggørelse eller videregivelse Afhængigt af de konkrete omstændigheder kan det være påkrævet, at den dataansvarlige myndighed eller virksomhed tager skridt til: at påse, at data bliver slettet eller eventuelt afhentet eller returneret fra uberettigede modtagere at sørge for at data slettes fra internet, herunder fra søgemaskiner at sørge for en hurtig underretning af berørte personer

at det langsigtet sikres, at situationen ikke gentager sig. F.eks. ved at interne retningslinjer og forretningsgange kigges efter, ved bedre instruktion af medarbejdere, og/eller ved systemteknisk understøttelse af relevante forretningsgange i organisationen.

Hvis den dataansvarlige har foretaget en eller flere af de ovenfor nævnte foranstaltninger, vil dette skulle angives i anmeldelsen til Datatilsynet. Ovennævnte liste er dog langt fra udtømmende for, hvilke skridt, der kan være relevante at træffe i forbindelse med et brud på persondatasikkerheden.

Det skal endelig bemærkes, at der ikke gælder specifikke formkrav til selve anmeldelsen, ligesom bestemmelsen heller ikke indeholder nogle sprogmæssige krav.

Der henvises imidlertid til afsnit 3.3.2., som beskriver den digitale indretningsløsning via hjemmesiden www.virk.dk, hvorigennem den dataansvarlige kan anmelde et brud på persondatasikkerheden til Datatilsynet.

3.5.2 Anmeldelse i faser

Det følger af databeskyttelsesforordningens artikel 33, stk. 4, at
"Når og for så vidt som det ikke er muligt at give oplysningerne samlet, kan oplysningerne meddeles trinvist uden unødig yderligere forsinkelse."

Som det fremgår af ovenstående tillader reglerne om anmeldelse af brud på persondatasikkerheden, at den dataansvarlige kan meddele Datatilsynet de fornødne oplysninger om bruddet ad flere omgange, hvis ikke det er muligt for den dataansvarlige at give alle oplysningerne på tidspunktet for den første indberetning.

Dette kan f.eks. være tilfældet, hvis der er tale om et omfattende brud på persondatasikkerheden, som nødvendiggør en større undersøgelse fra den dataansvarliges side for at kunne fastslå omfanget og de sandsynlige konsekvenser af bruddet.

Den dataansvarlige skal dog afgive så mange oplysninger om bruddet som muligt i sin første indberetning.

Det vil herudover ikke være i overensstemmelse med bestemmelsen at tilbageholde yderligere relevante oplysninger med henblik på at meddele dem samlet til Datatilsynet, idet oplysningerne skal gives uden unødig yderligere forsinkelse.

At den dataansvarlige ikke er i stand til at afgive alle de oplysninger, som er oplistet i bestemmelsens stk. 3, inden for tidsfristen på de 72 timer, kan desuden ikke udgøre en begrundelse for at fravige det overordnede krav om, at anmeldelse af bruddet skal ske til Datatilsynet inden for 72 timer.

3.5.3 Hvad nu, hvis anmeldelsen bliver forsinket?

Som tidligere omtalt under afsnit 3.3.1. er tidsgrænsen på de 72 timer for anmeldelse til Datatilsynet ikke definitiv, men overskrides fristen på 72 timer, skal anmeldelsen ledsages af en begrundelse for forsinkelsen.

Datatilsynet vil således, hvis der foreligger tungtvejende grunde hertil, kunne acceptere, at en anmeldelse er indgivet efter udløbet af fristen på 72 timer. Det påhviler imidlertid den dataansvarlige at løfte bevisbyrden for, at der foreligger tilstrækkeligt tungtvejende grunde, der umuliggjorde anmeldelse til Datatilsynet inden for 72 timer.

Eksempel:

3.5.4 "Samlet" anmeldelse i tilfældet af identiske brud på persondatasikkerheden

Som udgangspunkt skal hvert brud på persondatasikkerheden anmeldes særskilt til Datatilsynet. Dog vil den dataansvarlige være berettiget til at indgive en samlet anmeldelse for flere identiske brud på persondatasikkerheden, der omfatter de samme typer personoplysninger, og som finder sted inden for en relativt kort tidsperiode.

Hvis en serie af brud på persondatasikkerheden derimod vedrører forskellige typer af personoplysninger, der på forskellig vis er blevet kompromitteret, skal den dataansvarlige fortsat anmelde bruddene enkeltvist.

3.6 Intern dokumentation af brud på persondatasikkerheden

Det følger af databeskyttelsesforordningens artikel 33, stk. 5, at
" Den dataansvarlige dokumenterer alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet på persondatasikkerheden, dets virkninger og de trufne afhjælpende foranstaltninger. Denne dokumentation skal kunne sætte tilsynsmyndigheden i stand til at kontrollere, at denne artikel er overholdt."

Det vigtigste at være opmærksom på i forhold til dokumentationspligten er, at alle brud på persondatasikkerheden skal dokumenteres, uanset om den dataansvarlige er forpligtet til at anmelde bruddet til Datatilsynet.

Den dataansvarlige skal således føre et internt register over sine brud på persondatasikkerheden. Dette gælder også, selvom den dataansvarlige har vurderet, at bruddet ikke indebærer en risiko for fysiske personers rettigheder og frihedsrettigheder, jf. afsnit 3.1 ovenfor. For at være omfattet af dokumentationspligten er det dog en forudsætning, at det pågældende sikkerhedsbrud involverer personoplysninger således, at der er tale om *et brud på persondatasikkerheden*, jf. afsnit 2.1. ovenfor.

Dokumentationen skal, som det fremgår af bestemmelsen, sætte Datatilsynet i stand til at kontrollere, om den dataansvarlige har overholdt databeskyttelsesforordningens regler for anmeldelse af brud på persondatasikkerheden, herunder om den dataansvarlige har været berettiget til at undlade at foretage anmeldelse til tilsynet og/eller underrette de registrerede i medfør af artikel 34.

Der gælder dog ikke specifikke formkrav til dokumentationen, og den dataansvarlige kan derfor

Brud på persondatasikkerheden hos x- virksomhed eller myndighed:	Beskrivelse af bruddet:
1. Dato og tidspunkt for bruddet?:	
2. Hvad er der sket?:	
3. Årsagen til bruddet?:	
4. Hvilken type persondata 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?:	

selv beslutte, hvordan denne vil sikre den fornødne dokumentation i overensstemmelse med artikel 33, stk. 5. Det følger imidlertid af bestemmelsen, at dokumentationen skal indeholde en række informationer om bruddet, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne afhjælpende foranstaltninger.

Med inspiration i Artikel-29 gruppens beskrivelse af dokumentationspligten i forbindelse med brud på persondatasikkerheden, bør en fortegnelse over den dataansvarliges brud på persondatasikkerheden som minimum indeholde følgende oplysninger:

Som hjælp til udfyldelsen af fortegnelsen over den dataansvarliges brud på persondatasikkerheden, kan henvises til vejledningens bilag D, der bl.a. indeholder eksempler på typer af personoplysninger og mulige konsekvenser ved et brud på persondatasikkerheden. Den dataansvarlige kan i øvrigt overveje at supplere sin interne fortegnelse over brud med oplysninger fra blanketten i bilag D.

Der skal endvidere gøres opmærksom på, at en kopi af den dataansvarliges eventuelle anmeldelse af et brud på persondatasikkerheden til Datatilsynet, som er foretaget via den digitale indberetningsløsning på virk.dk, kan anvendes som dokumentation for bruddet i overensstemmelse med artikel 33, stk. 5. Dette forudsætter selvfølgelig, at anmeldelsesblanketten er udfyldt korrekt og tilstrækkeligt fyldestgørende.

3.7 Hvis bruddet har betydning for registrerede i flere EU-medlemslande?

Såfremt et brud på persondatasikkerheden indebærer en risiko for personer i andre EU-medlemslande, skal den dataansvarlige oplyse dette i forbindelse med indberetningen af bruddet til Datatilsynet.

Eksempel: En dansk virksomhed, der via deres hjemmeside tilbyder onlinesalg af lægemidler kommer ved en fejl til at lække en oversigt over virksomhedens seneste onlinesalg. Udover kundernes fulde navn, fremgår bl.a. betalings-, kontakt- og adresseoplysninger på kunderne. Virksomheden har mange kunder, der er bosat i andre EU-medlemslande, og ud fra den lækkede oversigt kan virksomheden konstatere, at kunder bosat i henholdsvis Spanien, Sverige og Tyskland har været berørt af lækagen. Såfremt betingelserne for anmeldelse til Datatilsynet er opfyldt i henhold til Databeskyttelseslovens § 33, skal virksomheden via anmeldelsen meddele Datatilsynet, at personer i de ovenfor angivne EU-medlemslande har været berørt.

Der gælder de samme betingelser for, hvornår et brud på persondatasikkerheden skal anmeldes til Datatilsynet, uanset om de berørte personer er bosat i andre EU-medlemslande.

Når Datatilsynet har modtaget meddelelse om, at personer i andre EU-medlemslande er berørt af et brud på persondatasikkerheden, er det Datatilsynets ansvar at underrette de relevante tilsynsmyndigheder i de respektive medlemslande.

4.0 Krav om anmeldelse til andre myndigheder i medfør af anden lovgivning

Ved et brud på persondatasikkerheden skal den dataansvarlige være opmærksom på, at der kan være pligt til at indberette sikkerhedsbrud, herunder brud på persondatasikkerheden i medfør af anden lovgivning.

Som eksempel herpå indeholder følgende lovgivninger en pligt til at indberette forskellige typer af sikkerhedsbrud til de relevante tilsynsmyndigheder:

- **Direktiv (EU) 2016/1148 af 6. juli 2016** om foranstaltninger, der skal sikre et højt fælles sikkerhedsniveau for net- og informationssystemer i hele Unionen (NIS-direktivet).

Efter reglerne i ovennævnte direktiv pålægges visse forsyningsvirksomheder og andre operatører af væsentlige tjenester samt udbydere af digitale tjenester at underrette de nationale myndigheder I tilfælde af væsentlige sikkerhedshændelser, der har væsentlige konsekvenser for de tjenester, der leveres/udbydes.

- **Forordning nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden**, jf. direktiv 2002/58/EF vedrørende databeskyttelse inden for elektronisk kommunikation.

Ovennævnte regelsæt forpligter udbydere af elektroniske kommunikationstjenester til at underrette Erhvervsstyrelsen om brud på persondatasikkerheden.

- **Direktiv (EU) 2015/2366 af 25. november 2015** om betalingstjenester i det indre marked.

Reglerne i dette direktiv pålægger udbydere af betalingstjenester at underrette Finanstilsynet om større drifts- og sikkerhedshændelser.

I tilfælde af spørgsmål til de enkelte indberetningsordninger henvises til de relevante indberetningsmyndigheder.

5.0 Underretning af den registrerede

5.1 Hvilke brud på persondatasikkerheden kræver underretning?

Det følger af databeskyttelsesforordningens artikel 34, stk. 1, at
" Når et brud på persondatasikkerheden sandsynligvis vil indebære en **høj** risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige uden unødig forsinkelse den registrerede om bruddet på persondatasikkerheden."

Som det følger af bestemmelsen, skal der ske underretning af den registrerede, når et brud på persondatasikkerheden sandsynligvis vil indebære **en høj risiko** for fysiske personers rettigheder og frihedsrettigheder. For så vidt angår den dataansvarliges bedømmelse af risikoen for fysiske personers rettigheder og frihedsrettigheder henvises til afsnit 3.1.2-3.1.4 ovenfor.
Den ovenfor nævnte underretning skal bl.a. ske med henblik på at give den registrerede mulighed for at træffe de fornødne forholdsregler i tilfælde af, at der er sket kompromittering af vedkommendes personoplysninger.

Pligten til i visse situationer at underrette de personer, der er berørt af et brud på persondatasikkerheden, adskiller sig dog fra reglerne om anmeldelse af brud på persondatasikkerheden til Datatilsynet, idet det efter artikel 34 forudsættes, at bruddet indebærer en **høj** risiko for de registrerede. Det må således antages, at omstændighederne omkring bruddet skal være yderligere skærpet i forhold til anmeldelsesforpligtelsen i artikel 33, førend kravet om underretning af de registrerede aktiveres. Det må samtidig kunne udledes heraf, at alle de brud på persondatasikkerheden, som kræver underretning af de registrerede, skal anmeldes til Datatilsynet.

5.1.1. "Høj" risiko

Som beskrevet ovenfor under afsnit 2.3. kan et brud på persondatasikkerheden medføre store skadevirkninger for de personer, der er berørt af bruddet – såsom diskrimination, identitetstyveri, eller -svindel, økonomisk tab, skade på omdømme, tab af fortrolighed af data underlagt tavshedspligt eller enhver anden økonomisk eller social ulempe for den registrerede.

Der findes ikke i databeskyttelsesforordningen en definition af betegnelsen "høj risiko". Men det må ved en vurdering af risikoens omfang, som tidligere anført under afsnit 3.1.3., lægges til grund, at jo mere *alvorlige* konsekvenser bruddet kan medføre, jo større vil risikoen være for de berørte personer. Tilsvarende vil en større *sandsynlighed* for, at et brud vil få konsekvenser for de registrerede ligeledes indebære en større risiko.

Som betingelsen "høj risiko" indikerer, må der antages at skulle foreligge en *nærliggende* risiko for, at et brud på persondatasikkerheden har eller kan få alvorlige konsekvenser for de berørte personer.

Hvis det dermed er sandsynligt, at et brud på persondatasikkerheden kan medføre alvorlige konsekvenser (såsom identitetstyveri, økonomisk tab mv.) skal den dataansvarlige underrette de registrerede med henblik på at give vedkommende mulighed for at varetage sine interesser og reducere risikoen for de negative følgevirkninger af bruddet.

Når det dataansvarlige skal foretage denne vurdering, bør den dataansvarlige tage alle de mulige konsekvenser og negative virkninger for den registrerede i betragtning. Dette omfatter således også de eventuelt "sekundære" konsekvenser for de registrerede, som et brud på persondatasikkerheden kan medføre.

Eksempel: Et onlinebaseret musikstreamingtjeneste med 5.000 brugere bliver hacket og dets brugerdatabase bliver i den forbindelse kopieret og offentliggjort på internettet.

Oplysningerne, som er blevet lækket, består af brugerens fulde navn samt brugernavn og adgangskode til tjenesten. De negative konsekvenser ved lækagen for de registrerede kan umiddelbart virke relativt harmløse.

Da mange brugere imidlertid anvender den samme adgangskode på forskelige konti, vil bruddet som en sekundær negativ virkning kunne medføre et brud på fortroligheden i forbindelse med en anden konto. De registrerede kunne minimere disse sekundære virkninger ved at skifte adgangskoden på alle deres andre konti.

Som følge heraf bør den dataansvarlige foretage underretning af de berørte personer med henblik at de kan træffe de fornødne forholdsregler, herunder ved at skifte adgangskoder på andre konti, hvis nødvendigt.

5.2. Situationer, hvor der ikke er krav om underretning

Idet risikoen for de registreredes rettigheder og frihedsrettigheder alt andet lige kan udledes at skulle være større end efter reglerne om anmeldelse af brud på persondatasikkerheden til Datatilsynet, kan det lægges til grund, at den dataansvarlige ikke skal underrette de registrerede, hvis den dataansvarlige har vurderet, at der ikke er pligt til at anmelde bruddet til Datatilsynet.

Det står dog den dataansvarlige frit for, om denne ønsker at underrette de registrerede uanset ,at der ikke er pligt hertil i henhold til databeskyttelsesforordningens artikel 34.

5.2.1. Hvis ikke bruddet indebærer en høj risiko

For det første, vil der *ikke* være krav om underretning, hvis ikke det er sandsynligt, at et brud på persondatasikkerheden vil indebære en **høj** risiko for fysiske personers rettigheder og frihedsrettigheder.

Eksempel på et brud, der **ikke** indebærer en høj risiko for de registrerede:

En kommune skal sende et svar via mail til en borger, der har søgt om tilladelse til at lave en tilbygning til sit hus.

Ved en fejl kommer en sagsbehandler hos kommunen til at vedhæfte en oversigt over alle de ejendomme, der har en versende sag om byggetilladelse hos kommunen. Af oversigten fremgår

alene information om ansøgernes navne, adresser samt kommunens sagsnummer. Der står oplistet 15 ejendomme på oversigten.

Kommunen bliver dagen efter kontaktet af borgeren, der gør kommunen opmærksom på fejlen. Det bliver aftalt, at borgeren med det samme sletter mailen, og at kommunen sender en ny mail med det korrekte indhold.

Underretning af de registrerede vil formentlig ikke være nødvendig henset til oplysningernes karakter og antallet af uberettigede modtagere (1 person).

Eksempel på et brud, der indebærer en høj risiko for de registrerede:

En kommune opretter samme dag en række sager i kommunens elektroniske byggesagsarkiv. Kommunen har imidlertid glemt at fjerne oplysninger om ansøgernes cpr-nummer i de uploadede dokumenter. Der er tale om 4 dokumenter tilhørende 4 forskellige byggesager.

Kommunen bliver opmærksom på fejlen 2 måneder efter, da en af de berørte borgere har fundet frem til dokumentet ved at søge på sit cpr-nummer via Google. Kommunen tjekker i den forbindelse de resterende 3 sager igennem.

I denne situation bør kommunen underrette de berørte personer om offentliggørelsen af deres cpr-numre. Dette henset til den tid oplysningerne har været tilgængelige via internettet samt den omstændighed, at et cpr-nummer vil kunne misbruges til bl.a. identitetstyveri. De registrerede skal derfor have mulighed fro at træffe deres forholdsregler som følge af offentliggørelsen.

Kommunen bør i den forbindelse vejlede de registrerede om, hvilke forholdsregler vedkommende kan træffe med henblik på at reducere risikoen for misbrug af oplysningerne.

5.2.2. Øvrige betingelser, som medfører, at der ikke er krav om underretning af de registrerede

Det følger af databeskyttelsesforordningens artikel 34, stk. 3, at
"Det er ikke nødvendigt at underrette den registrerede som omhandlet i stk. 1, hvis en af følgende betingelser er opfyldt:
***a)** den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger, og disse foranstaltninger er blevet anvendt på de personoplysninger, som er berørt af bruddet på persondatasikkerheden, navnlig foranstaltninger, der gør personoplysningerne uforståelige for enhver, der ikke har autoriseret adgang hertil, som f.eks. kryptering*
***b)** den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registreredes rettigheder og frihedsrettigheder som omhandlet i stk. 1 sandsynligvis ikke længere er reel*
***c)** det vil kræve en uforholdsmæssig indsats. I et sådant tilfælde skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde."*

5.2.2.1. Ad litra a
Som et eksempel på en situation, der kan give den dataansvarlige anledning til at vurdere, at underretning af de registrerede ikke er nødvendig, kan nævnes eksempel nr. 1 under afsnit 3.2.,

hvor en virksomheds personalechef får stjålet en ekstern harddisk, der er beskyttet med en stærk kryptering. Den dataansvarlige skal dog have en klar formodning om, at personoplysningerne er beskyttet på en sådan måde, at det er utænkeligt, at uvedkommende vil kunne få adgang til oplysningerne – f.eks. ved at komme i besiddelse af rette krypteringsnøgle.

Tilsvarende vil brugen af pseudonymisering, hvor direkte identificerbare personoplysninger erstattes med pseudonymer (”koder”) kunne medføre, at oplysningerne er beskyttet på en sådan måde, at det ikke umiddelbart er muligt at genkende vedkommende.

5.2.2.2. Ad litra b

Som et eksempel på en situation, hvor den høje risiko for de registrerede sandsynligvis ikke længere er reel som følge af den dataansvarliges efterfølgende foranstaltninger, kan henvises til eksempel nr. 2 under afsnit 3.2., hvor en medarbejder hos en kommune kommer til at uploade en fil på kommunens hjemmeside med fortrolige oplysninger. Medarbejderen bliver straks opmærksom på fejlen og fjerner filen fra hjemmesiden. Kommunens it-afdeling kan ved en undersøgelse af hjemmesidens log-oplysninger konstatere, at der ikke har været besøgende på hjemmesiden i det tidsrum, hvor filen har været eksponeret. Kommunen konkluderer samtidig, at der ikke er noget der tyder på, at filen er blevet kopieret af søgemaskiner, såsom Google.

5.2.2.3. Ad litra c

Som det fremgår af bestemmelsens litra c, vil den dataansvarlige kunne undlade at underrette de registrerede enkeltvis, såfremt det vil kræve *en uforholdsmæssig indsats.*

Der findes ikke i forordningen en klar definition af, hvornår betingelsen om uforholdsmæssig indsats er opfyldt, men det må antages, at den dataansvarlige, f.eks. henset til antallet af berørte personer, kan undlade at underrette de registrerede særskilt om et brud på persondatasikkerheden. Det må imidlertid bero på en konkret vurdering, som den dataansvarlige i første omgang er nærmest til at foretage.

Det kan ligeledes tænkes, at den dataansvarlige kan undlade at underrette de registrerede, hvis det viser sig, at være umuligt eller uforholdsmæssigt vanskeligt at tilvejebringe kontaktoplysninger på de registrerede.

I så fald vil den dataansvarlige, som det følger af bestemmelsen, i stedet skulle foretage en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Som et eksempel på en offentlig meddelelse kan f.eks. nævnes en meddelelse på den dataansvarliges hjemmeside, i et nyhedsbrev eller lignende sted, som forventes at blive set af de berørte personer.

Bevisbyrden for, at en af de ovennævnte betingelser er opfyldt, påhviler den dataansvarlige. Den dataansvarlige skal således være i stand til at begrunde, hvorfor underretning af de registrerede blev fravalgt.

Der kan endvidere i henhold til databeskyttelsesforordningens artikel 23, stk. 1, gøres undtagelser fra underretningspligten i artikel 34 ud fra et hensyn til bl.a. statens sikkerhed. Denne undtagelsesbestemmelse forventes dog at have et begrænset anvendelsesområde.

5.3. Tidspunktet for underretningen

5.3.1. Hvad siger reglerne?

Hvis det er sandsynligt, at et brud på persondatasikkerheden vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, underretter den dataansvarlige den registrerede uden unødig forsinkelse om bruddet på persondatasikkerheden.

Som det fremgår af bestemmelsen, indeholder denne ikke noget specifikt krav til, hvornår underretning af den registrerede skal ske.

Ligesom for kravet om anmeldelse til Datatilsynet, skal underretning ske uden unødig forsinkelse efter, at bruddet på persondatasikkerheden er påvist. Der henvises i den forbindelse til afsnit 3.3.3. ovenfor, der beskriver, hvornår den dataansvarlige anses for at være blevet "bekendt" med bruddet.

Kravet om underretning uden unødig forsinkelse skal bl.a. ses i sammenhæng med formålet med underretningen, som ifølge databeskyttelsesforordningen er at give den registrerede mulighed for at træffe de fornødne forholdsregler.

Af databeskyttelsesforordningen fremgår det endvidere, at underretningen til de registrerede bør gives, så snart det med rimelighed er muligt og i tæt samarbejde med tilsynsmyndigheden.

Det fremgår i den forbindelse, at behovet for at begrænse en umiddelbar risiko for skade kræver *omgående* underretning af registrerede, mens behovet for at gennemføre passende foranstaltninger mod fortsatte eller lignende brud på persondatasikkerheden kan begrunde en længere frist for underretning. Der henvises i øvrigt til afsnit 3.3. ovenfor.

5.4. Hvilke oplysninger skal meddeles?

5.4.1. Hvad siger reglerne?

> Det følger af databeskyttelsesforordningens artikel 34, stk. 2, at
> "Underretningen af den registrerede i henhold til denne artikels stk. 1 skal i et klart og forståeligt sprog beskrive karakteren af bruddet på persondatasikkerheden og mindst indeholde de oplysninger og foranstaltninger, der er omhandlet i artikel 33, stk. 3, litra b), c) og d)."

Som det følger af bestemmelsen, skal meddelelsen til de registrerede mindst indeholde følgende oplysninger:

> **1.** Karakteren af bruddet på persondatasikkerheden.
> **2.** Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
> **3.** De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
> **4.** 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.

Der er ligesom for anmeldelsespligten til Datatilsynet tale om en ikke-udtømmende opregning af, hvilke oplysninger der skal gives til den registrerede. Den dataansvarlige kan derfor beslutte at give den registrerede flere oplysninger i relation til bruddet end krævet efter artikel 34, stk. 2.

Idet der efter artikel 34, stk. 2, stilles de samme krav til indholdet af underretningen af de registrerede som efter reglerne om anmeldelse af et brud på persondatasikkerheden til Datatilsynet (artikel 33), henvises der til afsnit 3.5.1.1. – 3.5.1.4. ovenfor.

Sammen med beskrivelsen af de foranstaltninger, som den dataansvarlige har truffet for at håndtere bruddet, bør meddelelsen indeholde anbefalinger til den registrerede med henblik på at begrænse de mulige skadevirkninger.

5.4.2. Formkrav

Det fremgår endvidere af bestemmelsen, at de i stk. 2 angivne oplysninger, som skal meddeles de registrerede, skal gives i et klart og forståeligt sprog.

Hensigten bag denne skal igen ses i sammenhæng med selve formålet med at underrette de registrerede således, at disse har mulighed for at træffe det fornødne forholdsregler. Hvis underretningen ikke er tilstrækkelig klar og forståelig for modtageren, vil vedkommende have vanskeligt ved at træffe de nødvendige foranstaltninger med henblik på at reducere bruddets negative virkninger.

Når den dataansvarlige vil underrette den registrerede om et brud på persondatasikkerheden, bør den dataansvarlige derfor tage hensyn til modtageren og sikre sig, at meddelelsen er forståelig for vedkommende. Den dataansvarlige bør i den sammenhæng bl.a. tage hensyn til vedkommendes modersmål, sprogkundskaber, alder mv.

5.5. Hvordan skal den registrerede underrettes?

Den dataansvarlige skal underrette den registrerede direkte, f.eks. via e-mail, sms, brev eller lignende.

I tilknytning hertil beskriver Artikel 29-gruppen, at en meddelelse til den registrerede om et brud på persondatasikkerheden ikke bør sendes til vedkommende sammen med anden information, såsom generelle opdateringer, nyhedsbreve eller standard meddelelser fra den dataansvarlige. Ifølge artikel 29 gruppen understøtter dette, at formidlingen af bruddet bliver mere tydelig og gennemsigtig.

Udover underretning ved hjælp af direkte kommunikation til den registrerede (f.eks. via e-mail), nævner Artikel 29-gruppen bl.a. anvendelsen af fremtrædende website bannere eller meddelelser, samt annoncering i et trykt nyhedsmedie, som mulige metoder til at underrette de registrerede. Underretning af de registrerede, der alene består i en pressemeddelelse, vil ikke være tilstrækkelig for at opfylde underretningspligten i databeskyttelsesforordningens artikel 34.

Artikel 29-gruppen anbefaler i øvrigt, at den dataansvarlige benytter den metode til underretning af de registrerede, som giver størst chance for at meddelelsen om bruddet på persondatasikkerheden kommer frem til *alle* de berørte personer. Den dataansvarlige kan i den forbindelse overveje at benytte flere kommunikationsmetoder med henblik på at underrette de registrerede.

5.5.1. Hvis den registrerede er mindreårig (under 18 år)?

En meddelelse i henhold til artikel 34, bør **som hovedregel** først gives til børn og unge selv, når de er fyldt 15 år. Der lægges herved vægt på, at det almindeligvis må antages at forudsætte en vis alder at forstå indholdet af en sådan meddelelse. Det må endvidere antages, at alene sådanne større børn og unge er i stand til at varetage deres interesser i anledning af, at vedkommende er berørt af et brud på persondatasikkerheden. Det er ligeledes af betydning herfor, at en person under 15 år ofte må antages at have vanskeligt ved at forstå betydningen af en meddelelse i henhold til databeskyttelseslovens regler.

Underretningen skal i stedet gives til forældremyndighedsindehaveren.

For så vidt angår personer, der er fyldt 15 år, skal der som udgangspunkt tillige gives meddelelse til forældremyndighedsindehaveren. Det må dog bero på en vurdering i det konkrete tilfælde, om det er nødvendigt, at også forældremyndighedsindehaveren har viden om et brud på persondatasikkerheden, som vedkommendes barn er berørt af.

Meddelelsen til den mindreårige vil i en række tilfælde kunne gives i samme brev, mail eller lign., som meddelelsen til forældremyndighedsindehaveren. Forældremyndighedsindehaver vil derefter i givet fald normalt kunne give den mindreårige en forklaring om det skete, som er afpasset den pågældendes individuelle modenhed og indsigt.

Datatilsynet vil ikke udelukke, at der undtagelsesvis i konkrete tilfælde kan være forhold, som taler for at give særskilt meddelelse til børn og unge også under 15 år. Dette må bero imidlertid bero på en konkret vurdering, herunder om der er særlige hensyn til barnet/den unge, som nødvendiggør dette.

5.5.2. Hvem kan foretage underretning af de registrerede?

Som det fremgår af artikel 34, stk. 1, er det **den dataansvarlige**, der har ansvaret for at underrette de berørte personer om et brud på persondatasikkerheden.

Den dataansvarlige vil dog kunne uddelegere opgaven med at underrette de registrerede til en databehandler eller tredjemand efter bemyndigelse fra den dataansvarlige, f.eks. på baggrund af en fuldmagt.

5.6. Underretning efter krav fra Datatilsynet

> Det følger af databeskyttelsesforordningens artikel 34, stk. 4, at
> "Hvis den dataansvarlige ikke allerede har underrettet den registrerede om bruddet på persondatasikkerheden, kan tilsynsmyndigheden efter at have overvejet sandsynligheden for, at bruddet på persondatasikkerheden indebærer en høj risiko, kræve, at den dataansvarlige gør dette, eller beslutte, at en af betingelserne i stk. 3 er opfyldt."

Det følger således af bestemmelsens stk. 4, at Datatilsynet har beføjelse til at påbyde den dataansvarlige at underrette de registrerede om et brud på persondatasikkerheden, såfremt tilsynsmyndigheden vurderer, at bruddet sandsynligvis indebærer en høj risiko for de registrerede. Denne beføjelse er uafhængig af, om den dataansvarlige er enig med Datatilsynet i denne vurdering.

Det kan f.eks. ske, at den dataansvarlige i tilknytning til en anmeldelse af et brud på persondatasikkerheden til Datatilsynet begrunder sit fravalg af at underrette de registrerede, men at tilsynet ikke mener, at der er tilstrækkelige holdepunkter for den manglende underretning.

Omvendt kan Datatilsynet beslutte, at en af betingelserne i bestemmelsens stk. 3, er opfyldt, og at den dataansvarlige som følge heraf er undtaget fra underretningspligten i artikel 34.

6.0 Opsummering

- 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 i så fald underrette den registrerede **uden unødig** forsinkelse.

- Underretningen skal navnlig indeholde oplysninger om:

    1. Karakteren af bruddet på persondatasikkerheden.
    2. Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
    3. De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
    4. 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 skal gives i et klart og forståeligt sprog.

- 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.
- Datatilsynet kan kræve, at den dataansvarlige foretager underretning af de registrerede.

7.0 Implementering i organisationen

For at kunne sikre en effektiv efterlevelse af reglerne om anmeldelse til Datatilsynet og underretning af de registrerede bør den dataansvarlige (og databehandleren) udarbejde 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. Som nævnt under afsnit 3.4. kan dette bl.a. ske ved, at den dataansvarlige stiller krav om underretning af brud på persondatasikkerheden i databehandleraftalen.

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

- *Rapportering og vurdering af hændelsen, ansvarsfordeling, håndtering, evaluering og forbedring.*

Den dataansvarlige (og databehandlere) bør herudover overveje, hvilke tekniske og organisatoriske foranstaltninger, der kan indføres i organisationen for at sikre, at et brud på persondatasikkerheden bliver opdaget.

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 i henhold til databeskyttelseslovens artikel 33 og 34.
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.

8.0 Vil et anmeldt brud på persondatasikkerheden blive offentliggjort?

De indberettede anmeldelser af brud på persondatasikkerheden vil ikke blive offentliggjort af Datatilsynet.

Datatilsynet kan dog offentliggøre de eventuelle udtalelser og afgørelser, som tilsynet træffer i forlængelse af et brud på persondatasikkerheden. Datatilsynet vil dog udelade de informationer, som vil kunne kompromittere den dataansvarlige it-sikkerhed, forretningshemmeligheder eller lignende. (Databeskyttelseslovens § 33).

9.0 Bilag

A. **Flowchart**
B. **Oversigt – kravene til anmeldelse og underretning**
C. **Eksempler på brud på persondatasikkerheden og hvem der skal underrettes**
D. **Blanket til brug for anmeldelse til Datatilsynet**
E. **Blanket til brug for underretning af registrerede**