DATATILSYNET

Vejledning om håndtering af brud på person-datasikkerheden

Februar 2018

Indhold

1.0 Forord 3

2.0 Brud på persondatasikkerheden 4

2.1 Hvad er et brud på persondatasikkerheden? 4

2.2 Typer af brud på persondatasikkerheden 4

2.3 Hvad er de mulige konsekvenser af et brud på persondatasikkerheden? 5

3.0 Anmeldelse til Datatilsynet 6

3.1 Hvordan foretages anmeldelse til Datatilsynet? 6

3.2 Hvilke brud på persondatasikkerheden kræver anmeldelse? 6

3.3 Tidspunktet for anmeldelse? 9

3.4 Hvem anmelder til Datatilsynet? 11

3.5 Hvilke forpligtelser har databehandleren? 11

3.6 Hvilke oplysninger har Datatilsynet brug for? 12

3.7 Situationer, hvor anmeldelse til Datatilsynet ikke er nødvendig 14

3.8 Hvis bruddet indebærer en risiko for registrerede i flere EU-medlemslande? 15

4.0 Underretning af den registrerede 18

4.1 Hvilke brud på persondatasikkerheden kræver underretning? 18

4.2 Tidspunktet for underretningen 19

4.3 Hvilke oplysninger skal meddeles? 20

4.4 Hvordan skal den registrerede underrettes? 21

4.5 Hvem kan foretage underretning af de registrerede? 22

4.6 Situationer, hvor der ikke er krav om underretning 22

4.7 Underretning efter krav fra Datatilsynet 25

5.0 Ansvarlighed og intern dokumentation 27

6.0 Krav om anmeldelse til andre myndigheder i medfør af anden lovgivning 29

7.0 Implementering i organisationen 30

8.0 Opsummering 31

9.0 Bilag A – Flowchart 32

10.0 Bilag B – eksempler på brud og hvem der skal underrettes 33

1.0 Forord

Når databeskyttelsesforordningen finder anvendelse i Danmark og resten af EU fra den 25. maj 2018, vil der – som noget nyt – gælde en generel forpligtelse for alle dataansvarlige til som udgangspunkt at anmelde brud på persondatasikkerheden til Datatilsynet. Anmeldelsen skal ske uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet. Samtidig fastsættes der en forpligtelse, som allerede i dag tolkes ud af persondatalovens grundregel om god databehandlingsskik og Datatilsynets praksis, til som udgangspunkt at underrette de registrerede i tilfælde af brud på persondatasikkerheden.

Begge forpligtelser er udtryk for databeskyttelsesforordningens fokus på ansvarlighed, når det kommer til at overholde databeskyttelsesreglerne. Reglerne har til formål at tilvejebringe gennemsigtighed og især at sikre, at dataansvarlige reagerer, når der opstår et brud på persondatasikkerheden.

Det skal i tilknytning hertil nævnes, at hvis reglerne om anmeldelse af brud på persondatasikkerheden og underretning af de registrerede ikke overholdes, har Datatilsynet en række korrigerende beføjelser. Tilsynet kan f.eks. udtale kritik eller udstede et påbud. Afhængigt af omstændighederne i hver enkelt sag 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.

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/underretning om et sikkerhedsbrud, ligesom der i vejledningen vil blive redegjort for forordningens krav til tidspunktet for, hvornår der skal ske anmeldelse/underretning, og måden hvorpå anmeldelsen skal indgives til Datatilsynet.

Ønskes en nærmere gennemgang af reglerne, henvises der bl.a. til selve lovteksten i databeskyttelsesforordningens kapitel IV, afdeling 2 (Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger) samt afsnittene 5.11. og 5.12. i betænkning nr. 1565/2017 om databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning.

Artikel 29-gruppen (fremover Det Europæiske Databeskyttelsesråd) har også offentliggjort en vejledning om underretning af brud på persondatasikkerheden ("Guidelines on personal data breach notification under Regulation 2016/679") (WP 250 rev 01). Vejledningen kan findes på www.datatilsynet.dk.

Det bemærkes, at vejledningen vil blive opdateret, når forslaget til den nye databeskyttelseslov er vedtaget.

2.0 Brud på persondatasikkerheden

2.1 Hvad er et brud på persondatasikkerheden?

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

Et brud på persondatasikkerheden er samtidig en informationssikkerhedshændelse. Dette begreb er i ISO 27000-standarden defineret 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 …"

Det er kun de *informationssikkerhedshændelser,* 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.

En informationssikkerhedshændelse vil således ikke altid være et brud på persondatasikkerheden. 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.

2.2 Typer af brud på persondatasikkerheden

Et brud på persondatasikkerheden kan f.eks. rent teknisk ske, når den dataansvarliges it-systemer med personoplysninger ikke er tilstrækkelig sikret, således at udefrakommende får adgang til oplysningerne (f.eks. hacking). Det kan imidlertid også være den dataansvarliges egen håndtering af personoplysningerne, der kan forårsage et brud, f.eks. hvis den dataansvarlige ubeføjet videregiver eller ændrer personoplysningerne. Et andet eksempel, når det gælder den dataansvarliges egen håndtering af personoplysningerne er, hvis den dataansvarlige ulovligt eller som følge af et hændeligt uheld (f.eks. brand eller oversvømmelse) i en periode ikke har adgang til eller ender med at tilintetgøre personoplysningerne.

Som eksempler på brud på persondatasikkerheden kan nævnes:

1) Andre personer end den eller de personer hos dataansvarlige, der er autoriseret til det, får (uautoriseret) adgang til personoplysninger. Det kan både være personer uden for eller inden for dataansvarliges organisation.

2) Den dataansvarliges medarbejdere ændrer eller sletter personoplysninger ved et uheld.
3) Brud på den dataansvarliges server, hvor uvedkommende har fået indsigt i personoplysninger – f.eks. kundedatabasens CPR-oplysninger, kreditkortoplysninger el.lign.
4) Den dataansvarliges medarbejdere videregiver ubevidst eller bevidst personoplysninger om en borger/kunde til en anden borger/kunde – eller måske ligefrem flere andre uvedkommende personer.
5) Når manglede kryptering af den dataansvarliges hjemmeside indeholdende f.eks. et kundelogin resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.

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

I databeskyttelsesforordningen er nævnt en række eksempler på, hvilke konsekvenser et brud på persondatasikkerheden kan have for fysiske personer.

Et brud kan, hvis det ikke håndteres på en passende og rettidig måde, 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 for den berørte fysiske person.

Relevante bestemmelser mv.

Forordningens artikel 4, nr. 12
Præambelbetragtning nr. 75, 85 og 86.

3.0 Anmeldelse til Datatilsynet

3.1 Hvordan foretages anmeldelse til Datatilsynet?

For at gøre det nemt og enkelt for virksomheder og myndigheder at indberette sikkerhedshændelser på databeskyttelsesområdet og en række andre områder, arbejdes der i øjeblikket på at etablere én fælles digital løsning for anmeldelser af sikkerhedshændelser. Initiativet skal understøtte, at virksomhederne og myndighederne kun skal indberette hændelser én gang, ét sted frem for at skulle indberette stort set samme information flere steder.

Løsningen placeres på **Virk.dk**, som allerede i dag er den digitale indgang for virksomheder og myndigheder i forhold til indberetninger til det offentlige.

Der etableres en intelligent indberetningsløsning, som kan håndtere forskellige myndigheders krav til information og som gennem de spørgsmål, der stilles, kanaliserer indberetningerne hen til den eller de rette myndighed(er).

Den digitale indberetningsløsning vil være tilgængelig, når databeskyttelsesforordningen finder anvendelse fra den 25. maj 2018. Det vil til den tid også 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 blanket, som skal udfyldes af den dataansvarlige. 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 3.6.

3.2 Hvilke brud på persondatasikkerheden kræver anmeldelse?

Som udgangspunkt skal alle brud på persondatasikkerheden anmeldes til Datatilsynet. Det er således kun, hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, at der ikke skal ske anmeldelse.

> En risiko for fysiske personers rettigheder og frihedsrettigheder omfatter bl.a. 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.

Det skal i tilknytning hertil nævnes, at manglende efterlevelse af reglerne om anmeldelse af brud på persondatasikkerheden til Datatilsynet kan resultere i, at Datatilsynet f.eks. udtaler kritik eller udsteder et påbud til den dataansvarlige. Afhængigt af omstændighederne i hver enkelt sag 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.

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.

Der er tale om en *konkret* og *reaktiv* risikovurdering *specifikt* i forhold til konsekvenserne af bruddet på persondatasikkerheden.

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

De samme forhold, der bør indgå i den reaktive vurdering af risikoen ved et persondatasikkerhedsbrud, kan med fordel indgå i det proaktive risikobaserede arbejde, der er forudsat i databeskyttelsesforordningens bestemmelse om persondatasikkerhed (artikel 32) i forbindelse med, at der gennemføres passende tekniske og organisatoriske foranstaltninger, og i forordningens bestemmelse om udarbejdelse af konsekvensanalyser (artikel 35).

Følgende forhold bør altid indgå i den konkrete vurdering af risikoen for de registreredes rettigheder og frihedsrettigheder som følge af et brud på persondatasikkerheden:

- Typen af sikkerhedsbrud, herunder om der er sket tab af oplysninger, brud på fortroligheden eller en integritetskrænkelse;
- Oplysningernes art og omfang;
- Risikoen for at registrerede kan identificeres;
- Konsekvenser bruddet kan have for de registrerede;
- Hvorvidt bruddet omfatter særlige registrerede (f.eks. hvis der er tale om børn eller særligt udsatte);
- Antallet af berørte fysiske personer;

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 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.

Oplysningernes art og omfang

Som udgangspunkt vil *oplysningernes art* have indflydelse på risikovurderingen. Jo mere følsomme personoplysninger, der er tale om, jo større konsekvenser må et sikkerhedsbrud formodes at få for de berørte personer. F.eks. må en utilsigtet 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 offentliggjort.

Det er dog i den forbindelse vigtigt at holde sig for øje, at alle omstændigheder omkring sikkerhedsbruddet skal tages 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 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

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 følsomme personoplysninger 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.

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 ved at matche oplysningerne med anden information, vil kunne identificere den pågældende.

Det vil i den sammenhæng kunne få betydning, hvis den dataansvarlige har beskyttet oplysningerne ved f.eks. at anvende kryptering eller pseudonymisering[1], da det som følge heraf ikke umiddelbart vil være muligt at identificere vedkommende.

Alvorligheden af konsekvenserne for de berørte personer

Som beskrevet i afsnit 2.3 ovenfor er der i databeskyttelsesforordningen nævnt en række eksempler på, hvilke konsekvenser et brud på persondatasikkerheden kan have for fysiske personer.

Herudover vil et brud, der forårsager kompromittering af oplysninger om særligt sårbare eller udsatte personer, kunne vurderes at have større skadevirkning. Det samme vil 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 ske anmeldelse til Datatilsynet. Den dataansvarlige bør dog være sikker i sin sag, når modtagerens troværdighed tillægges betyd-

[1] 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.

ning 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 der f.eks. sker et læk af en persons betalingskortoplysninger 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 omstændigheder ved den registrerede

Som nævnt ovenfor kan det få betydning for risikovurderingen, hvis der er tale om oplysninger om 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 f.eks. være tilfældet, hvis der 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, og hvilke behandlingsaktiviteter denne foretager sig, kan også 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 helbredsoplysninger i stort omfang, eller et kreditoplysningsbureau, der behandler oplysninger om personer, 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.

Relevante bestemmelser mv.

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

3.3 Tidspunktet for anmeldelse?

Hvis det er sandsynligt, 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.

Bekendt med, at der er sket et brud

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*.

Alene formodningen om, at et brud på persondatasikkerheden har fundet sted, vil i den forbindelse ikke være tilstrækkeligt til at anse et brud på persondatasikkerheden for at være "sket".

En sådan 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, ligesom det kan være en anledning til at overveje sikkerheden omkring behandlingen af personoplysninger.
I vurderingen af, om der er "sket" et brud på persondatasikkerheden, kan der også lægges vægt på, om de oplysninger, som den dataansvarlige 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 nedenfor i afsnit 3.6.

Uden unødig forsinkelse og om muligt senest 72 timer efter bruddet

En anmeldelse om et brud på persondatasikkerheden skal som udgangspunkt ske *uden unødig forsinkelse og om muligt senest 72 timer efter bruddet*.

Den dataansvarlige er med andre ord 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 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.

Når det gælder tidsgrænsen på de 72 timer, tages der ved vurderingen af, hvorvidt den er overholdt ikke hensyn til, at den dataansvarlige måske først bliver bekendt med bruddet uden for normal kontortid, herunder i weekender og på helligdage.

De 72 timer for anmeldelse til Datatilsynet er dog ikke en absolut frist. Forordningen tillader således, at den dataansvarlige først anmelder et brud på persondatasikkerheden efter udløbet af fristen på de 72 timer. Anmeldelsen skal i så fald 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 gøres i den forbindelse endvidere opmærksom på muligheden for at meddele de oplysninger, der skal ledsage anmeldelsen, trinvist til Datatilsynet, se nærmere afsnit 3.6 nedenfor.

Relevante bestemmelser mv.

Forordningens artikel 33, stk. 1
Præambelbetragtning nr. 85

3.4 Hvem anmelder til Datatilsynet?

Som udgangspunkt er det den dataansvarlige, som anmelder 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, og at dette fremgår af den databehandleraftale, der er indgået mellem parterne, se også afsnit 3.5. nedenfor.

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.

Relevante bestemmelser mv.

Forordningens artikel 33, stk. 1
Præambelbetragtning nr. 85

3.5 Hvilke forpligtelser har databehandleren?

Bliver en eventuel databehandler opmærksom på, at der er sket et brud på persondatasikkerheden, har databehandleren pligt til uden unødig forsinkelse at underrette den dataansvarlige om bruddet.

Der er tale om en absolut forpligtelse, dvs. 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 bør også ske underretning af 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 derfor i sin vejledning af 3. oktober 2017 om underretning af brud på persondatasikkerheden[2], 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. Databehandlerens pligt til 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 sørge for at meddele detaljerne om bruddet individuelt til hver dataansvarlig.

Det bemærkes, at det skal fremgå af databehandleraftalen mellem den dataansvarlige og databehandleren, at databehandleren – under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren – skal bistå den dataansvarlige med at sikre overholdelse af forpligtelserne i medfør af bl.a. artikel 33 om anmeldelse af brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet), jf. forordningens artikel 28, stk. 3, litra f.

Relevante bestemmelser mv.

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

3.6 Hvilke oplysninger har Datatilsynet brug for?

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

[2] Artikel 29-gruppens vejledning om underretning af brud på persondatasikkerheden (WP 250 rev 01).

- 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.

De oplysninger, som 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 Datatilsynet overvejer at gøre brug af sine korrigerende beføjelser til midlertidigt eller definitivt at begrænse, herunder forbyde en behandling.

Der er tale om en ikke udtømmende liste over indholdet af informationer, og opregningen ovenfor udelukker dermed ikke, at den dataansvarlige afgiver yderligere informationer for at sikre, at forpligtelsen til at anmelde brud på persondatasikkerheden er overholdt.

Den dataansvarlige må således gerne forsyne Datatilsynet med eventuelle andre yderligere informationer, hvis dette vurderes formålstjenligt - ligesom tilsynet naturligvis også vil kunne kræve yderligere oplysninger af den dataansvarlige efterfølgende, hvis dette er nødvendigt i forbindelse med behandlingen af anmeldelsen. Hvis den dataansvarlige skal forklare (og Datatilsynet skal forstå) omstændighederne omkring et brud ordentligt, kan det således være nødvendigt med yderligere informationer.

I afsnit 3.1. ovenfor er en nærmere omtale af den fælles digitale indretningsløsning via hjemmesiden www.virk.dk, der er under etablering, og hvorigennem bl.a. den dataansvarlige kan anmelde et brud på persondatasikkerheden til Datatilsynet.

Relevante bestemmelser mv.

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

At den dataansvarlige ikke er i stand til at afgive alle de oplysninger, der som minimum skal med i anmeldelsen, inden for tidsfristen på de 72 timer, kan ikke udgøre en begrundelse for at fravige det overordnede krav om, at anmeldelse af bruddet skal ske til Datatilsynet inden for 72 timer. Den dataansvarlige må i stedet afgive oplysninger trinvist til Datatilsynet uden yderligere forsinkelse.

Når forordningen indeholder denne mulighed, skal det ses i lyset af, at det kan tage tid at afdække de relevante oplysninger, f.eks. 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. Delvise oplysninger i en situation med brud på persondatasikkerheden anses i en sådan situation for at være bedre for Datatilsynets handlemuligheder end ingen information.

Den dataansvarlige skal dog afgive så mange oplysninger om bruddet som muligt i sin første anmeldelse. Den dataansvarlige må således ikke tilbageholde yderligere relevante oplysninger

med henblik på at meddele dem samlet til Datatilsynet, idet oplysningerne skal gives uden unødig yderligere forsinkelse.

Relevante bestemmelser mv.

Forordningens artikel 33, stk. 4

3.7 Situationer, hvor anmeldelse til Datatilsynet ikke er nødvendig

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.

Eksempel: 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 5.0.

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 på denne måde 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: 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 logoplysninger 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 kunders rettigheder eller frihedsrettigheder.

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.

3.8 Hvis bruddet indebærer en risiko for registrerede i flere EU-medlemslande?

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

En dansk virksomhed kan således behandle oplysninger ikke bare om fysiske personer i Danmark, men også om fysiske personer, der befinder sig i andre EU-medlemslande. Der findes også virksomheder i Danmark, som udelukkende behandler oplysninger om fysiske personer, der befinder sig i andre EU-medlemslande.

Der gælder i sådanne situationer de samme betingelser for, hvornår et brud på persondatasikkerheden skal anmeldes til tilsynsmyndigheden.

Forordningens bestemmelser om, hvilken tilsynsmyndighed i EU's medlemslande der er kompetent til at behandle anmeldelsen indebærer imidlertid, at den kompetente myndighed til at modtage og behandle den dataansvarliges anmeldelse af bruddet på persondatasikkerheden ikke i alle tilfælde vil være Datatilsynet i Danmark.

Den kompetente myndighed er således 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[3]. Det betyder med andre ord, at når et brud på sikkerheden omhandler oplysninger om fysiske personer i mere end ét EU-medlemsland, og der skal ske anmeldelse, vil den dataansvarlige skulle foretage anmeldelse til den ledende tilsynsmyndighed.

Dataansvarlige virksomheder med grænseoverskridende behandlinger skal derfor foretage en vurdering af, hvilken tilsynsmyndighed blandt EU's medlemslande, der er ledende tilsynsmyndighed for den.

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

Hvis den dataansvarlige ikke har nået at foretage en vurdering af, hvilken tilsynsmyndighed der er ledende tilsynsmyndighed for den – eller er i tvivl om, hvorvidt dens vurdering er korrekt, bør den som minimum sørge for at underrette den "lokale" tilsynsmyndighed i det land, hvor bruddet på persondatasikkerheden er sket.

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

Hvis den dataansvarlige vælger **kun** at anmelde et brud på persondatasikkerheden til den ledende tilsynsmyndighed, anbefales det, at den dataansvarlige, når det er relevant, sørger for at indikere over for tilsynsmyndigheden, at bruddet omfatter etableringer i andre EU-medlemslande og i hvilke EU-medlemslande, der er fysiske personer, der er berørt af bruddet. Når den ledende tilsynsmyndighed – det kan f.eks. være Datatilsynet i Danmark – har modtaget anmeldelsen, herunder oplysningerne om, at fysiske 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.

---

[3] Se i den forbindelse også Artikel 29-gruppens vejledning om identifikation af den dataansvarliges eller databehandlerens ledende tilsynsmyndighed (WP 244 rev.01).

Eksempel: En virksomhed med hovedvirksomhed i Danmark tilbyder via sin hjemmeside onlinesalg af håndkøbsmedicin. Ved en fejl kommer virksomheden til på hjemmesiden – i forbindelse med en opdatering af siden – 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-medlemslande, og ud fra den offentliggjorte oversigt kan virksomheden konstatere, at et antal kunder bosat i henholdsvis 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.

Relevante bestemmelser mv.

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

4.0 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. Gør den dataansvarlige ikke dette, har Datatilsynet mulighed for at gå ind i sagen og kræve, at den dataansvarlige foretager underretning af den registrerede.

Formålet med underretningen er bl.a. at give den registrerede mulighed for at træffe de fornødne forholdsregler i tilfælde af, at der er sket kompromittering af vedkommendes personoplysninger.

Som beskrevet ovenfor under afsnit 2.3. kan et brud på persondatasikkerheden medføre store skadevirkninger for de personer, der er berørt af bruddet – så som 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 begrebet "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.

Når den dataansvarlige skal foretage denne risikovurdering, bør alle de mulige konsekvenser og negative virkninger for den registrerede tages i betragtning. Dette omfatter således også de eventuelt "sekundære" konsekvenser for de registrerede, som et brud på persondatasikkerheden kan medføre (se eksempel nedenfor).

Den dataansvarlige skal endvidere, afhængigt af de sandsynlige negative virkninger, foretage underretning, uanset antallet af berørte registrerede.

Eksempel: En musikstreamingtjenestes websted er blevet hacket, og dets brugerdatabase er blevet stjålet og offentliggjort på internettet. De lækkede personoplysninger består af brugernes fulde navn, musikpræferencer samt brugernavn og adgangskode til tjenesten for de brugere, der har registreret sig på tjenestens hjemmeside. 9.000 brugere er berørt.

De negative konsekvenser ved lækagen for de registrerede kan umiddelbart virke relativt harmløse og kan give anledning til at overveje, om de registrerede skal underrettes. Da adgangskoderne er blevet kompromitteret, skal de dog fornyes af den dataansvarlige. I denne proces vil det være nødvendigt at informere brugerne om årsagen til, at adgangskoderne skal fornyes. Eftersom mange brugere anvender den samme adgangskode på forskellige konti, vil bruddet som en sekundær negativ virkning sandsynligvis også medføre et brud på fortroligheden i forbindelse med en anden konto. De registrerede vil kunne minimere disse sekundære virkninger ved at skifte adgangskoden på alle deres andre konti. Underretningen skal derfor også indeholde oplysninger om de sandsynlige negative virkninger i forbindelse med andre konti og bør derfor omfatte en anbefaling om at bruge forskellige adgangskoder på forskellige websteder og om at forny adgangskoderne til konti, hvor den kompromitterede adgangskode blev anvendt.

Eksempel: En kommune får i forbindelse med, at en række sager i kommunens offentligt tilgængelige elektroniske byggesagsarkiv skal oprettes, ved en fejl ikke fjernet oplysninger om ansøgernes personnummer i de uploadede dokumenter. Der er tale om 4 dokumenter fra 4 forskellige byggesager. Kommunen bliver først opmærksom på fejlen 2 måneder efter, da en af de berørte borgere har fundet frem til dokumentet ved at søge på sit personnummer via Google. Kommunen tjekker i den forbindelse de andre sager i byggesagsarkivet igennem og finder frem til de 3 andre sager, hvor der er begået samme fejl.

Kommunen vil være forpligtede til at underrette de berørte personer om offentliggørelsen af deres personnumre. Dette henset til den tid oplysningerne har været tilgængelige via internettet samt den omstændighed, at et personnummer vil kunne misbruges til bl.a. identitetstyveri. De registrerede skal derfor have mulighed for at træffe deres forholdsregler som følge af offentliggørelsen. Kommunen bør i den forbindelse endvidere vejlede de registrerede om, hvilke forholdsregler vedkommende kan træffe med henblik på at reducere risikoen for misbrug af oplysningerne.

4.2 Tidspunktet for underretningen

Den dataansvarlige skal underrette den registrerede **uden unødig forsinkelse** efter, at bruddet på persondatasikkerheden er påvist. Underretningen afhænger ikke af tidspunktet for, hvornår der sker anmeldelse af bruddet til Datatilsynet.

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

Det fremgår i den forbindelse også af forordningen, at underretninger til de registrerede bør gives, så snart det med rimelighed er muligt.

Eksempelvis kan behovet for at begrænse en umiddelbar risiko for skade kræve *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.

Eksempel: Der er sket et brud på persondatasikkerheden og den registreredes beskyttede fysiske adresse er blevet offentliggjort. Adressen er beskyttet, fordi den registrerede risikerer fysisk vold fra en anden person. Det kan her være af afgørende betydning, hvornår den registrerede får underretning om offentliggørelsen.

Eksempel: Mange mennesker bruger den samme kombination af brugernavn og adgangskode til mange internetkonti, og er disse oplysninger blevet kompromitteret i forbindelse med et brud på persondatasikkerheden hos en dataansvarlig, således at tredjemand nu kender oplysningerne, vil tredjemanden sandsynligvis kunne få adgang til andre konti tilhørende den pågældende registrerede, herunder i nogle tilfælde e-mailkonto. Konsekvenserne for den registrerede kan i et sådant tilfælde eventuelt begrænses, jo hurtigere vedkommende underrettes om bruddet på persondatasikkerheden med en klar anbefaling om at ændre adgangskoder til alle de konti, der deler den samme kompromitterede adgangskode.

Relevante bestemmelser mv.

Forordningens artikel 34, stk. 1
Præambelbetragtning nr. 86

4.3 Hvilke oplysninger skal meddeles?

Underretningen til den registrerede skal beskrive karakteren af bruddet på persondatasikkerheden og som minimum:

- 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.

Som i relation til selve anmeldelsen af bruddet på persondatasikkerheden til Datatilsynet, er der tale om en ikke-udtømmende opregning af, hvilke oplysninger der skal gives til den registrerede, jf. ordet ”minimum”.

Den dataansvarlige kan derfor beslutte at give den registrerede yderligere oplysninger om bruddet, så længe underretningen fortsat er klar og let forståelig. Se nærmere umiddelbart nedenfor og afsnit 4.4.

Hvis det er relevant, bør den dataansvarlige også give den registrerede specifikke råd om, hvordan den registrerede kan beskytte sig mod mulige negative konsekvenser af bruddet, som f.eks. nulstilling eller ændring af adgangskoder, hvis den registreredes adgangsoplysninger er blevet kompromitteret.

Underretningen af den registrerede skal gives i et klart og forståeligt sprog.

Kravet skal ses i sammenhæng med selve formålet med at underrette den registrerede om bruddet på persondatasikkerheden. Hvis underretningen ikke er tilstrækkelig klar og forståelig for den registrerede, 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.

Den dataansvarlige må endvidere ikke afkræve den registrerede nogen form for betaling for underretningen eller de foranstaltninger, den dataansvarlige måtte have truffet for at beskytte den registreredes rettigheder og frihedsrettigheder.

4.4 Hvordan skal den registrerede underrettes?

Hvordan underretning mest hensigtsmæssigt foretages, skal vurderes i forhold til det skete brud på persondatasikkerheden. Den dataansvarlige skal underrette den registrerede direkte, 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.

Eksempel: Et realkreditinstitut havde fremsendt årsopgørelser, der var modtageren uvedkommende. Af årsopgørelserne fremgik oplysninger om navn, adresse, personnummer samt oplysninger om låneforhold. Instituttet kontakter pr. brev 74 af de 75 personer, om hvem der er udsendt oplysninger til uvedkommende. Den sidste berørte modtager havde man været i telefonisk dialog med. Af brevskabelonen, som instituttet benyttede sig af, fremgår det, at der alene blev orienteret om, at den udsendte årsopgørelse var forkert. Meddelelsen indeholdt således ikke oplysning om, at der havde været et brud på persondatasikkerheden, som havde medført, at kundens oplysninger var gjort tilgængelige for uvedkommende.

Underretningen til de registrerede er mangelfuld. Set i lyset af omstændighederne i sagen bør realkreditinstituttet informere de berørte personer om bruddet, herunder at oplysninger om deres kundeforhold er sendt til uvedkommende. Der lægges herved vægt på, at de oplysninger, som er sendt til uvedkommende omfatter navn, adresse, personnummer samt oplysninger om låneforhold. Der er således tale om ganske omfattende oplysninger, og det kan ikke udelukkes, at det skete ville kunne få konkrete konsekvenser for de berørte.

Artikel 29-gruppen anbefaler i øvrigt i sin vejledning af 3. oktober 2017 om underretning af brud på persondatasikkerheden[4], 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.

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.

Den dataansvarlige vil dog kunne uddelegere opgaven med at underrette de registrerede til en databehandler eller tredjemand. Dette forudsætter imidlertid, at databehandleren eller tredjemand har fået bemyndigelse hertil, f.eks. på baggrund af en fuldmagt. Når det gælder databehandleren bør denne forpligtelse til at foretage underretning af de registrerede dog også fremgå af den databehandleraftale, der er indgået mellem parterne, se også afsnit 3.5.ovenfor.

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

Relevante bestemmelser mv.

Forordningens artikel 34, stk. 2

4.6 Situationer, hvor der ikke er krav om underretning

Hvis bruddet ikke indebærer en høj risiko

Hvis den dataansvarlige efter at have foretaget en vurdering af alle de mulige konsekvenser og negative virkninger for de registrerede af et brud på persondatasikkerheden når frem til, at bruddet er af en sådan karakter, at det sandsynligvis ikke vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder, er det ikke nødvendigt at underrette den registrerede.

Eksempel: En kommune skal sende et svar via e-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 verserende 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 e-mailen, og at kommunen sender en ny mail med det korrekte indhold.

[4] Artikel 29-gruppens vejledning om underretning af brud på persondatasikkerheden (WP 250 rev 01).

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

Bevisbyrden for, at ovennævnte betingelse er opfyldt, påhviler den dataansvarlige. Den dataansvarlige skal således f.eks. i forbindelse med en sag hos Datatilsynet være i stand til at begrunde, hvorfor underretning af den registrerede blev fravalgt.

Der er gennemført passende tekniske og organisatoriske foranstaltninger

Hvis den dataansvarlige efter at have foretaget en vurdering af alle de mulige konsekvenser og negative virkninger for de registrerede af et brud på persondatasikkerheden når frem til, at bruddet er af en sådan karakter, at det sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder eller frihedsrettigheder, vil udgangspunktet være, at der skal ske underretning af den registrerede.

Det vil imidlertid ikke være nødvendigt at underrette den registrerede, hvis 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,

Som et **eksempel** på, hvad der kan give den dataansvarlige anledning til at vurdere, om underretning af de registrerede ikke er nødvendig under henvisning til, at ovennævnte betingelse er opfyldt, kan nævnes en situation, hvor en dataansvarlig har mistet et bærbart medie, hvorpå der er lagret personoplysninger i krypteret form. Der kan være anvendt en tilstrækkelig stærk kryptering, som ikke kan brydes eller omgås inden for en tilstrækkelig lang årrække, og uvedkommende har ikke og får ikke mulighed for at dekryptere data på normal vis – f.eks. ved at komme i besiddelse af rette krypteringsnøgle. Den dataansvarlige kan i så fald siges at have en formodning om, at personoplysningerne er beskyttet på en sådan måde, at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Bevisbyrden for, at ovennævnte betingelse er opfyldt, påhviler den dataansvarlige. Den dataansvarlige skal således f.eks. i forbindelse med en sag hos Datatilsynet være i stand til at begrunde, hvorfor underretning af den registrerede blev fravalgt.

Den høje risiko for de registrerede er sandsynligvis ikke længere reel

Hvis den dataansvarlige har truffet efterfølgende foranstaltninger, 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.

Som et **eksempel** på, hvad der kan give den dataansvarlige anledning til at vurdere, om underretning af den registrerede kan undlades, kan nævnes en situation, hvor et it-system opdateres, og denne opdatering resulterer i, at der utilsigtet etableres adgang til følsomme personoplysninger fra internettet, uden login (dvs. uden autorisation af brugeren). Herved bliver der i et tidsrum mulig adgang for uautoriserede personer til personoplysninger fra internettet. Den dataansvarlige opdager selv efterfølgende, at bruddet på persondatasikkerhed er sket og afskærer herefter straks adgangen for uautoriserede brugere, så personoplysningerne ikke længere er ekspone-

ret. Endvidere iværksætter den dataansvarlige straks en undersøgelse af de nærmere omstændigheder ved bruddet på persondatasikkerheden. Undersøgelsen dokumenterer med sikkerhed, i hvilket tidsrum data har været tilgængelige for uautoriserede personer. Undersøgelsen dokumenterer også, at der findes troværdige logs, som ikke kan omgås og som har logget, når personoplysninger blev tilgået i tidsrummet, hvor personoplysningerne var eksponeret. Det kan endvidere på grundlag af de troværdige logoplysninger dokumenteres, at kun autoriserede brugere faktisk har tilgået personoplysninger, mens de var eksponeret – dvs. i det tidsrum, hvor bruddet på persondatasikkerheden stod på.

Bevisbyrden for, at ovennævnte betingelse er opfyldt, påhviler den dataansvarlige. Den dataansvarlige skal således f.eks. i forbindelse med en sag hos Datatilsynet være i stand til at begrunde, hvorfor underretning af den registrerede blev fravalgt.

Kræver en uforholdsmæssig indsats

Den dataansvarlige vil endelig også kunne undlade at underrette de registrerede enkeltvis, hvis det i det konkrete tilfælde vil kræve *en uforholdsmæssig indsats.*

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. I hvilket omfang individuel underretning af registrerede personer er uforholdsmæssigt vanskelig eller endog umulig skal afgøres i den enkelte situation.

Som eksempel på et tilfælde, som umiddelbart må anses for at være omfattet af denne undtagelse, kan nævnes en situation, hvor en virksomhed har mistet rådigheden over alle kundeoplysninger i forbindelse med, at virksomhedens kundedatabase er blevet ramt af ransomware.

Hvis denne afvejning falder ud til, at det vil kræve en uforholdsmæssig indsats af den dataansvarlige at foretage underretning til hver enkelt registrerede, vil der i stedet skulle foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Bevisbyrden for, at ovennævnte betingelse er opfyldt, påhviler den dataansvarlige. Den dataansvarlige skal således f.eks. i forbindelse med en sag hos Datatilsynet være i stand til at begrunde, hvorfor underretning af den registrerede blev fravalgt.

Udsættelse af underretningen i henhold til national lovgivning

Regeringen har den 25. oktober 2017 **fremsat** et **forslag** til en **ny databeskyttelseslov (L 68)** for Folketinget. Loven skal erstatte den nugældende persondatalov og supplere databeskyttelsesforordningen.

Lovforslaget indeholder bl.a. en regel [5]om, at kravet om underretning af brud på persondatasikkerheden til den registrerede i enkelttilfælde kan suspenderes, så længe en underretning af den registrerede konkret må antages at vanskeliggøre efterforskningen af strafbare forhold.

[5] Lovforslagets § 22, stk. 6

Reglen forudsætter, at politiet f.eks. som led i en anmeldelse af et strafbart forhold - eksempelvis omfattet af straffelovens § 193 om forhold, der fremkalder omfattende forstyrrelse i driften af bl.a. informationssystemer - er blevet bekendt med, at et brud på persondatasikkerheden har fundet sted. I det omfang politiet konkret vurderer, at en underretning af de berørte registrerede ville vanskeliggøre den videre efterforskning, vil politiet kunne træffe beslutning om at underretningspligten skal udsættes over for den eller de berørte dataansvarlige.

Reglen er alene tiltænkt et begrænset anvendelsesområde og forudsætter, at der foretages en samlet vurdering, hvor der tages hensyn til de - til dels modstridende - interesser og hensyn, der er knyttet til efterforskningen af det relevante strafbare forhold, omfanget og karakteren af bruddet på persondatasikkerheden samt antallet af berørte registrerede.

I det omfang politiet konkret finder, at en underretning af de registrerede ikke bør finde sted, vil der alene være tale om en udsættelse af den dataansvarliges underretningsforpligtelse. Politiet vil således være forpligtede til løbende at vurdere, hvornår en underretning vil kunne finde sted samt til at fremme efterforskningen, bevissikringen mv. med henblik på at begrænse perioden, hvor underretningen er udsat mest muligt. Det forventes, at der i reglen ikke vil være behov for at udsætte underretning i mere end få dage eller uger.

Det bemærkes, at en beslutning om udsættelse alene kan træffes af politiet, hvorfor en dataansvarlig, der egenhændigt afdækker en brist på persondatasikkerheden vil være henvist til at indgive politianmeldelse herom, hvorefter bestemmelsen vil kunne bringes i anvendelse, hvis politiet vurderer, at betingelserne herfor er opfyldt.

Beslutning efter bestemmelsen træffes af den politikreds, der forestår efterforskningen.

Relevante bestemmelser mv.

Forordningens artikel 23 og 34, stk. 3
Præambelbetragtning nr. 88
Forslag nr. L 68 af 25. oktober 2017 til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)

4.7 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. Adgangen 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 begrunder sit fravalg af at underrette den registrerede. Hvis Datatilsynet mener, at der ikke er tilstrækkelige holdepunkter for den manglende underretning, vil tilsynet meddele den dataansvarlige, at der skal ske underretning.

Datatilsynet kan imidlertid også nå frem til, at der foreligger en af de situationer, som er nævnt ovenfor under afsnit 4.5., og at den dataansvarlige som følge heraf ikke behøver foretage underretning af den registrerede.

Det skal i tilknytning hertil nævnes, at den dataansvarliges (og databehandlerens) manglende efterlevelse af reglerne om underretning af de registrerede kan resultere i, at Datatilsynet f.eks. udtaler kritik eller udsteder et påbud. Afhængigt af omstændighederne i hver enkelt sag 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

5.0 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 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.

Af Artikel 29-gruppens vejledning fra oktober 2017 om underretning af brud på persondatasikkerheden[6] fremgår det, at der stilles ikke 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 ifølge Artikel 29-gruppen 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 bruddet, er nået frem til, at det ikke skal anmeldes til tilsynsmyndigheden (Datatilsynet). Dokumentationen bør således i relation til denne beslutning omfatte en nærmere redegørelse for, hvorfor den dataansvarlige mener,

[6] Artikel 29-gruppens vejledning om underretning af brud på persondatasikkerheden (WP 250 rev 01).

at bruddet sandsynligvis ikke vil medføre en risiko for fysiske personers rettigheder og frihedsrettigheder.

Tilsvarende 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.

Eksempel på internt 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

6.0 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 sikkerhedsbrud, herunder brud på persondatasikkerheden, til andre myndigheder i medfør af anden lovgivning:

- Siden 2011 har telesektoren og virksomheder, som er omfattet af den særlige telelovgivning, været underlagt en pligt til at underrette (anmelde) **Erhvervsstyrelsen** om brud på persondatasikkerheden, jf. § 8 i lov om elektroniske kommunikationsnet og -tjenester[7] og bekendtgørelse nr. 462 af 23. maj 2016 om persondatasikkerhed i forbindelse med udbud af offentlige elektroniske kommunikationstjenester.

  Reglerne gennemfører dele af bl.a. Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om databeskyttelse inden for elektronisk kommunikation, som ændret ved Europa-Parlamentets og Rådets direktiv 2009/136/EF af 25. november 2009 (e-databeskyttelsesdirektivet) i dansk ret. Kommissionen har endvidere udstedt forordning nr. 611/2013 af 24. juni 2013 om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden. De nævnte EU-regler er i øjeblikket er under revision[8].

- **Center for Cybersikkerhed** har ressortansvaret for informationssikkerhed og beredskab i telesektoren. Ifølge loven om net- og informationssikkerhed[9] og den dertil hørende bekendtgørelse nr. 566 af 1. juni 2016 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed har udbydere af offentligt tilgængelige net og tjenester siden 1. juli 2016 været forpligtet til at foretage underretning til centret ved brud på informationssikkerheden, der har væsentlige følger for driften af net eller tjenester.

- **Finanstilsynet** forventer at blive orienteret om væsentlige it-hændelser hos finansielle virksomheder og fælles datacentraler. Endvidere stiller lov om betalinger[10] krav om, at udbydere af betalingstjenester snarest muligt skal underrette Finanstilsynet om større drifts- og sikkerhedshændelser, jf. § 127, stk. 1 i samme lov. De nærmere krav til, hvad indberetningen skal indeholde, fremgår af EBA's retningslinjer om rapportering af væsentlige it-hændelser.

I tilfælde af spørgsmål om ovenstående øvrige anmeldelsespligter henvises til de relevante ansvarlige myndigheder.

[7] Lovbekendtgørelse nr. 128 af 7. februar 2014, som ændret ved lov nr. 1567 af 15. december 2015.
[8] Se Kommissionen den 10. januar 2017 har fremsat et forslag til Europa-Parlamentets og Rådets forordning om respekten for privatlivet og beskyttelse af personoplysninger i forbindelse med elektronisk kommunikation og om ophævelse af direktiv 2002/58/EF (forordning om privatlivets fred og elektronisk kommunikation) (KOM/2017/010 endelig).
[9] Lov nr. 1567 af 15. december 2015 om net- og informationssikkerhed.
[10] Lov nr. 652 af 8. juni 2017 om betalinger.

7.0 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 og 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.

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.

8.0 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**.

- **Databehandleren** skal underrette den dataansvarlige om et brud **uden unødig forsinkelse**.

- 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:**

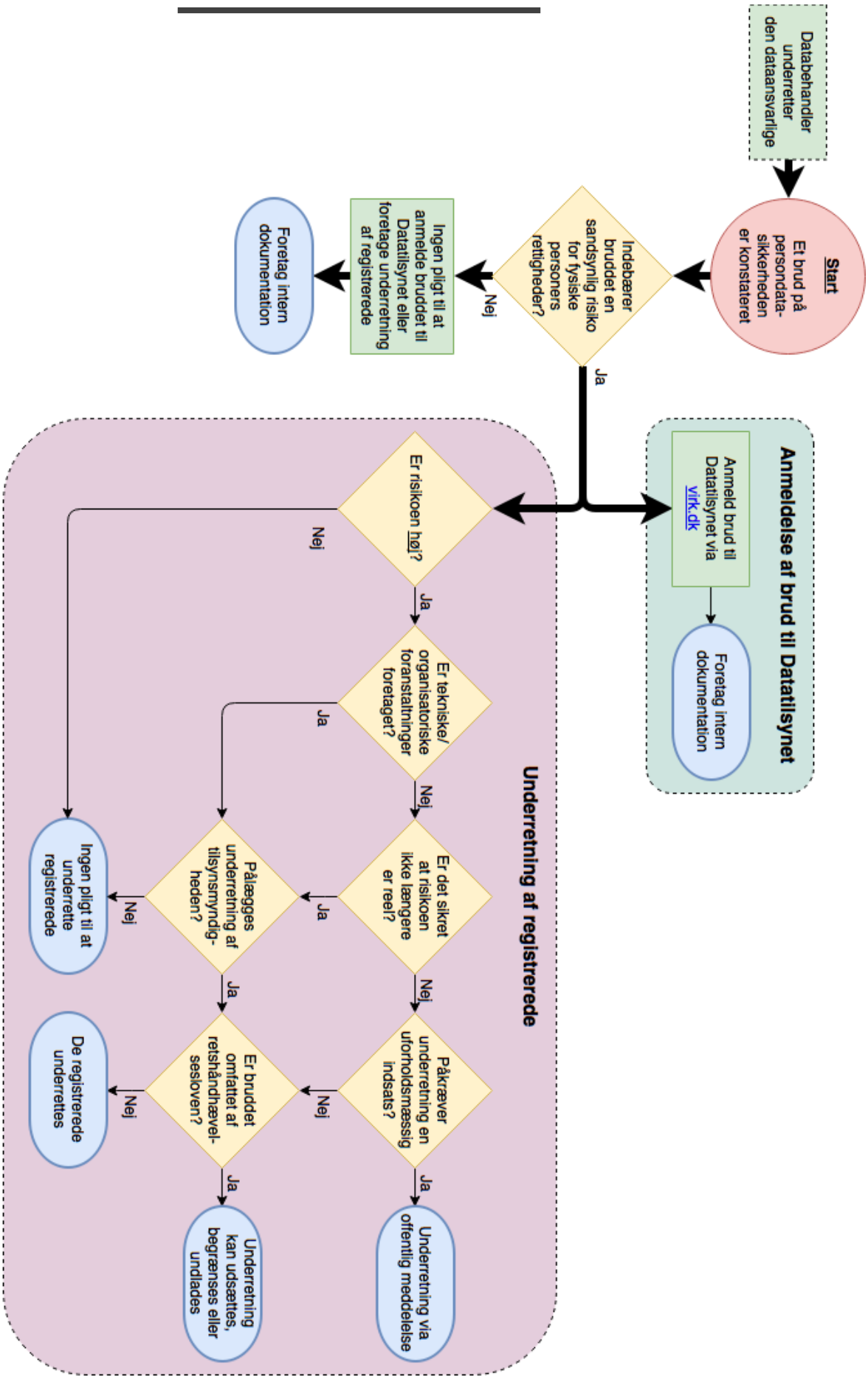
    - Navn på og kontaktoplysninger for databeskyttelsesrådgiveren eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes.
    - De sandsynlige konsekvenser af bruddet på persondatasikkerheden.
    - De foranstaltninger, som den dataansvarlige har truffet eller foreslår truffet for at håndtere 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.

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

9.0 Bilag A – Flowchart



10.0 Bilag B – eksempler på brud og hvem der skal underrettes

Eksempel	Skal der ske anmeldelse til Datatilsynet?	Skal den registrerede underrettes?
1. En medarbejder i en kommunes økonomiforvaltning bliver opmærksom på at vedkommende via kommunens elektroniske sagsbehandlingssystem (ESDH) har adgang til en sag, der behandles i kommunens socialforvaltning.	Ikke nødvendigvis. Kommunen kan vurdere, at bruddet ikke indebærer en risiko for de registrerede. Dette kan skyldes: 1. At der er tale om et "internt" brud på persondatasikkerheden og 2. At kommunen har stor tillid til den pågældende medarbejder og 3. At kommunen har gennemgået systemets logoplysninger og konstateret, at medarbejderen er den eneste, der har haft uberettiget adgang til oplysningerne.	Hvis kommunen vurderer, at der ikke er pligt til at underrette Datatilsynet, vil der heller ikke være pligt til at underrette den registrerede.
2. I forbindelse med besvarelsen af en aktindsigtsanmodning hos Ankestyrelsen kommer en medarbejder til at ligge de forkerte sagsakter i brevkuverten. Dokumenterne indeholder fortrolige og følsomme oplysninger om en anden person, herunder personnummer, oplysning om beregning af førtidspension samt oplysninger om vedkommendes helbred. Ankestyrelsen er ikke op-	Ja, der skal som udgangspunkt ske anmeldelse til Datatilsynet. Dette skyldes bl.a., at oplysningerne er kommet uvedkommende til kendskab, og at der er tale om personoplysninger af fortrolig og følsom karakter. Styrelsen skal underrette Datatilsynet uanset, at styrelsen har sørget for at hente dokumenterne tilbage fra den forkerte modtager.	Ja, styrelsen bør underrette den registrerede om, at oplysninger om ham/hende er kommet uvedkommende til kendskab. Dette er igen begrundet i typen af oplysninger, som er blevet videregivet og læst af en uberettiget modtager. Den registrerede skal således have mulighed for at træffe de fornødne forholdsregler.

mærksom på fejlen inden brevkuverten bliver modtaget hos den person, der har søgt om aktindsigt. Det er modtageren, der orienterer styrelsen om de forkerte sagsakter.		
3. En klinik for fysioterapi bliver udsat for ransomware, da en medarbejder trykker på et link i en e-mail, som er modtaget i klinikkens indbakke. Dette resulterer i, at al klinikkens data, herunder helbredsoplysninger om patienterne bliver krypteret og låst for klinikkens medarbejdere. Bagmændene kræver et større pengebeløb for at frigive oplysningerne. Klinikken har foretaget backup af sine systemer, men det er også lykkes bagmændene at kryptere disse. Klinikken har i deres systemer oplysninger om ca. 200 patienter, herunder oplysninger om patienternes diagnoser.	Ja, klinikken bør anmelde hændelsen til Datatilsynet. Dette skyldes bl.a., at uvedkommende potentielt kan have fået adgang til følsomme oplysninger vedrørende et stort antal personer, og at klinikken ikke vil have mulighed for at gendanne oplysningerne via deres backup kopi. Klinikken bør underrette Datatilsynet uanset, at det lykkes klinikken af få frigivet oplysningerne.	Ja, klinikken bør formentlig underrette de registrerede. Udover karakteren af de oplysninger, som er blevet ramt af angrebet, kan det muligvis få negative konsekvenser for de berørte personer, at oplysninger om et behandlingsforløb eller lign. hos klinikken ikke kan gendannes.
4. Et hospital rammes af et strømnedbrud, der varer i ca. 20 minutter, hvor det ikke er muligt at tilgå hospitalets it-systemer, herunder elektroniske patientjournaler.	Ikke nødvendigvis. Hvis strømnedbruddet viser sig ikke at have haft konsekvenser for hospitalets patienter – f.eks. fordi journalerne også opbevares fysisk – vil det ikke være nødvendigt at anmelde hændelsen til Datatilsynet.	Ikke nødvendigvis. Hvis ikke den manglende adgang til systemerne har haft konsekvenser for de berørte patienter, vil det ikke være nødvendigt at foretage underretning af disse.
5. En privat forsker i tarmkræft sender via e-mail en række testresultater til en forsker i	Det er ikke nødvendigt at anmelde bruddet til Datatilsynet.	Nej, det vil formentlig ikke være nødvendigt at underrette de registrerede, idet

USA. Forskeren har sørget for at pseudonymisere alle de personhenførbare oplysninger. Forskeren får imidlertid indtastet den forkerte mailadresse og mailen ender hos en forkert modtager.	Dette skyldes, at der er tale om pseudonymiserede oplysninger, og at det derfor ikke umiddelbart vil være muligt at identificere de berørte personer. Forskeren bør dog stadig sikre sig, at oplysningerne bliver destrueret hos den uberettigede modtager.	bruddet – pga. pseudonymiseringen – ikke indebærer en høj risiko for de registrerede.
6. På grund af en systemfejl er det muligt at få adgang til et universitets intranet uden brug af adgangskode og password. Via intranettet kan man bl.a. få oplyst, hvem der er indskrevet som elev på universitetet og disse personers e-mailadresser. Der er på tidspunktet indskrevet 36.000 elever på universitetet. Der har været adgang til intranettet uden adgangskode i ca. 2 uger. Elever med navne- og adressebeskyttelse fremgår ikke på intranettet.	Det kan være nødvendigt at anmelde bruddet til Datatilsynet. Henset til antallet af berørte personer og det tidsrum, hvor der har været adgang uden brug af kode, kan universitetet være forpligtet til at underrette Datatilsynet om bruddet. Hvis universitet imidlertid vurderer, at bruddet – henset til karakteren af de oplysninger, der har været uberettiget adgang til – ikke indebærer en risiko for de berørte personer, kan universitetet indlade at underrette Datatilsynet.	Hvis universitetet vurderer, at der ikke er krav om anmeldelse til Datatilsynet, vil det heller ikke være nødvendigt at underrette de berørte elever. Universitetet kan dog overveje i stedet at orientere elverne om hændelsen i form af en meddelelse på universitetets hjemmeside.
7. En online spiludbyder bliver udsat for et hackerangreb, der resulterer i, at virksomheden bl.a. får stjålet oplysninger om sine kunder, herunder oplysninger om navn, adresse og personnummer	Ja, spiludbyderen skal anmelde bruddet til Datatilsynet. Dette skyldes, at oplysninger om navn, adresse og personnummer bl.a. kan misbruges til at begå identitetstyveri, og at bruddet derfor formodes at indebære en risiko for de berørte personer.	Ja, spiludbyderen skal underrette de berørte personer. Da en oplysning om navn, adresse og personnummer kan misbruges til identitetstyveri, skal de registrerede have mulighed for at træffe foranstaltninger, der kan nedbringe risikoen for at oplysningerne bliver misbrugt.

8. Et hospital bliver af en sygeplejerske gjort opmærksom på, at en læge ansat hos hospitalet har tilegnet sig adgang til sin nabos patientjournal via hospitalets systemer. Lægen har fået nys om, at naboen er ramt af sygdom, og lægen er derfor nysgerrig efter at få at vide, hvad naboen fejler. Der er således ingen behandlingsrelation mellem lægen og naboen.	Ja, hospitalet skal som udgangspunkt anmelde bruddet til Datatilsynet. Dette skyldes bl.a., at oplysningerne er kommet uvedkommende til kendskab, og at der er tale om personoplysninger af fortrolig og følsom karakter.	Ja, hospitalet bør underrette den pågældende nabo om, at oplysninger om ham/hende er kommet uvedkommende til kendskab. Dette er igen begrundet i typen af oplysninger, som er tilgået af en uvedkommende person. Den registrerede skal således have mulighed for at træffe de fornødne forholdsregler.
9. En kommune vil sende et brev vedrørende nabovarsel om stor fest i nabolaget. Ved en fejl sender kommunen via digital post brevet til en forkert borger. Brevet indeholder den oprindelige borgers navn og adresse. Borgeren der modtager brevet gør straks kommunen opmærksom på fejlen. Kommunen aftaler skriftligt med borgeren der har modtaget brevet, at vedkommende sletter det.	Det vil formentlig ikke være nødvendigt at anmelde bruddet til Datatilsynet. Henset til oplysningernes karakter og da kommunen har tillid til, at brevet er blevet slettet, kan kommunen vurdere, at bruddet ikke indebærer en risiko for den registrerede.	Hvis kommunen vurderer, at der ikke er pligt til at underrette Datatilsynet, vil der heller ikke være pligt til at underrette den registrerede.

10. En HR-medarbejder sender ved en fejl lønsedler og ansættelseskontrakt til en forkert medarbejder i virksomheden. Det aftales, at medarbejderen sletter dokumenterne med det samme efter at være blevet opmærksom på fejlen.	Ikke nødvendigvis. Virksomheden kan vurdere, at bruddet ikke indebærer en risiko for den registrerede. Dette kan skyldes, at der er tale om et "internt" brud på persondatasikkerheden og, at virksomheden har stor tillid til den pågældende medarbejder.	Hvis virksomheden vurderer, at der ikke er pligt til at underrette Datatilsynet, vil der heller ikke være pligt til at underrette den registrerede.
11. Et lille flyttefirma har alle oplysninger om deres medarbejdere liggende på en computer, der ikke har backup. Computeren bliver ramt af vandskade, og oplysningerne kan ikke gendannes. På computeren lå bl.a. oplysninger om flere medarbejderes helbredsoplysninger.	Hvis virksomheden kan sikre de registreredes rettigheder af anden vej end elektronisk, skal virksomheden ikke anmelde bruddet. I modsat fald der ske anmeldelse til Datatilsynet.	Idet den enkelte medarbejder skal kunne varetage sine interesser, skal der ske underretning af medarbejderne. Det er den enkelte medarbejder der er nærmest til vurdere, om det, der er gået tabt, er blevet reetableret fyldestgørende.
12. En virksomhed har alle oplysninger om deres medarbejdere, inkl. personnumre og helbredsoplysninger, liggende på en computer. Computeren stjæles under et indbrud. Oplysningerne er ikke krypterede, men der skal almindeligt kodeord til for at låse computeren op.	Ja, virksomheden skal anmelde bruddet til Datatilsynet. Dette skyldes, at der er tale om følsomme og fortrolige personoplysninger om medarbejderne og, at der med de af virksomheden beskedne sikkerhedsforanstaltninger er en risiko for, at uvedkommende får adgang til personoplysningerne.	Ja, virksomheden bør underrette hver medarbejder om bruddet, idet der er stor sandsynlighed for, at oplysningerne kan blive kompromitteret. Den registrerede skal således have mulighed for at træffe de fornødne forholdsregler