VEJLEDNING

HÅNDTERING AF DATABRUD

**Definition af databrud:**

Et brud på datasikkerheden defineres i Databeskyttelsesforordningen som *”et brud på sikkerheden, der fører til ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet”.*

Eksempler på databrud kan være:

* Hackerangreb
* Ransomware
* Sletning af personoplysninger ved et uheld
* Fremsendelse af oplysninger i u-krypteret form, hvor der stilles krav om kryptering
* Tyveri eller bortkomst af hardware

**Håndtering af databrud:**

En konkret procedure for håndtering af databrud bør (ifølge ISO27001) være:

* Rapportering om databruddet internt i virksomheden eller organisationen samt en ansvarsfordeling for håndteringen af databrud
* Standarder for, hvad der skal til for at stoppe et databrud
* Hvordan vurderingen af risikoen som følge af bruddet skal foretages
* Procedure for hvem og hvordan der skal foretages anmeldelse til Datatilsynet og underretning til den registrerede
* Standarder for den nødvendige dokumentation af brud på datasikkerheden (*se evt. Enkel-GDPRs Skema til registrering af databrud*)

**Ansvarlighed og intern dokumentation:**

Det er et krav, at den dataansvarlige skal dokumentere alle brud, der sker på persondatasikkerheden. Herunder de faktiske omstændigheder ved bruddet, bruddets virkninger og de trufne foranstaltninger.

Den dataansvarlige er kun forpligtiget til at udlevere disse dokumentationer, hvis Datatilsynet anmoder herom. Pligten gør det derfor muligt for Datatilsynet at kontrollere, at anmeldelsespligten ved databrud overholdes. Derudover hænger kravet sammen med forordningens overordnede princip om ansvarlighed.

Der er ikke nogen formkrav for denne dokumentation. Dokumentationen skal dog i alle tilfælde indeholde en række informationer. Disse informationer vedrører:

* Dato og tidspunkt for bruddet
* Hvad der skete i forbindelse med bruddet
* Årsagen til bruddet
* Hvilke typer af personoplysninger som har været omfattet af bruddet
* Hvilke konsekvenser som bruddet har for de berørte registrerede
* Hvilke afhjælpende foranstaltninger, der er truffet
* Hvorvidt der er sket anmeldelse til Datatilsynet eller ej

Derudover bør dokumentationen indeholde en begrundelse for alle de væsentlige beslutninger, som er truffet som følge af bruddet. F.eks. hvis den dataansvarlige er kommet frem til, at der ikke bør ske anmeldelse til Datatilsynet, så skal denne vurdering vedlægges i dokumentationen. Det samme gælder, hvis det er vurderet, at der ikke bør ske underretning til den registrerede.

(*se Enkel-GDPRs Skema til registrering af databrud*)

**Anmeldelse til Datatilsynet:**

Når der sker et databrud, skal dette, som udgangspunkt, altid anmeldes til Datatilsynet. En sådan anmeldelse skal ske uden unødig forsinkelse – og senest 72 timer efter at den dataansvarlige er blevet bekendt med databruddet.

Det er udgangspunktet efter forordningen, at alle brud på datasikkerheden skal anmeldes. Men hvis det vurderes, at det er usandsynligt, at bruddet vil indebære en risiko for den registreredes rettigheder og frihedsrettigheder, skal et sådant brud ikke anmeldes til Datatilsynet. Hvorvidt der foreligger en risiko må vurderes i forhold til de mulige konsekvenser.

Undlades databruddet at blive anmeldt til Datatilsynet, kan Datatilsynet udtale kritik eller give et påbud til den dataansvarlige. Efter omstændighederne kan manglende efterlevelse af anmeldelsespligten føre til, at Datatilsynet pålægger den dataansvarlige en bøde.

For at finde ud af, om den dataansvarlige er forpligtiget til at anmelde et brud på datasikkerheden, skal den dataansvarlige omgående vurdere, hvorvidt bruddet medfører en risiko for den/de registrerede fysiske personers rettigheder. Dette skal ske så snart den dataansvarlige opdager databruddet.

En risikovurdering skal derfor foretages med udgangspunkt i de konsekvenser, der kan forekomme for de berørte parter som følge af et databrud. Til forskel fra andre risikovurderinger og konsekvensanalyser (*se Enkel-GDPRs vejledninger herom*), skal denne vurdering tage udgangspunkt i risikoen for de berørte registrerede og i risikoen som specifikt er opstået grundet bruddet på datasikkerheden.

Ifølge Datatilsynets vejledning om brud på datasikkerheden, skal følgende faktorer altid medregnes i den konkrete vurdering af risikoen i tilfælde af databrud:

Typen af datasikkerhedsbrud:

Typen af sikkerhedsbrud skal altid angives – hertil om der er sket brud på fortroligheden, tab af oplysninger eller andet. Konsekvenserne ved et databrud afhænger af, hvilken type af brud, der er tale om, og det er derfor meget vigtigt, at der angives præcist hvilken type af brud, der er tale om.

Oplysningernes beskaffenhed og omfanget af bruddet:

Personoplysningernes beskaffenhed eller art kan have betydning for vurderingen af risikoen. Brud på datasikkerheden bestående af følsomme personoplysninger, vil uomtvisteligt medføre en større risiko for den registrerede end et brud på almindelige personoplysninger (*se Enkel-GDPRs vejledning om Personoplysninger og behandling heraf i step 1*). Andre hensyn vedrørende personoplysningens art kan også have indflydelse på vurderingen af risikoen og bør derfor indgå i denne vurdering.

Omfanget af bruddet vil ligeledes kunne have en betydning for vurderingen af risikoen. Mængden af personoplysninger, som er berørt, skal dermed også inddrages. Det samme gælder den tidsmæssige udstrækning af et brud.

Risikoen for at registrerede kan identificeres:

I vurderingen af risikoen kan det også have en betydning, hvor nemt det vil være at identificere den/de fysiske person(er), som er blevet genstand for bruddet, gennem de pågældende oplysningerne eller ved en sammenligning af andre oplysninger, der i sin helhed vil gøre det muligt at identificere det enkelte individ. Det kan f.eks. have betydning om personoplysningerne har været krypterede eller pseudonymiserede, da det i et sådant tilfælde vil være vanskeligt at identificere personen.

Konsekvenser for den/de registrerede:

Konsekvenserne, som nævnt tidligere, kan variere meget alt efter omstændighederne ved det enkelte brud. Herudover vil et brud vedrørende personoplysninger om særligt udsatte eller sårbare personer kunne have større konsekvenser - f.eks. hvis der tale om børn.

Hvorvidt den dataansvarlige er bevidst om, hvor personoplysningerne præcist er endt, eller hvem der efter bruddet er kommet i besiddelse af personoplysningerne, kan også spille en rolle i forhold til de medførte konsekvenser.

Er det tilfældet, at personoplysningerne er af længerevarende eller permanent karakter, og dermed ikke let kan afhjælpes, vil konsekvenserne alt andet lige vurderes som værende betydeligt større, end hvis dette ikke var tilfældet. Altså vurderes det, om der kan foretages rimelige foranstaltninger for at reducere konsekvenserne betydeligt.

Om bruddet omfatter særlige registrerede:

Det bør samtidig inkluderes i risikovurderingen, hvorvidt oplysningerne vedrører et barn eller en anden sårbar person. Andre omstændigheder kan foreligge ved den registrerede, der kan have indflydelse på konsekvenserne ved bruddet for individet – og disse omstændigheder skal derfor også angives i risikovurderingen.

Antallet af fysiske personer, som er blevet berørt af bruddet:

Jo flere personer, som er berørt af et databrud – jo større vil risikoen for omfattende konsekvenser oftest være. Derfor skal antallet af berørte personer altid angives i anmeldelsen.

72-timersfristen:

Den dataansvarliges anmeldelse til Datatilsynet skal ske uden unødigt ophold og så vidt muligt 72 timer efter den dataansvarlige er blevet opmærksom på bruddet. Hvis en anmeldelse til Datatilsynet først sker efter 72 timer, skal anmeldelsen vedlægges en begrundelse for denne forsinkelse. Det vil sige, at fristen på 72 timer ikke er en absolut frist. Det tillades efter forordningen, at der sker senere anmeldelse, men i så fald er det et krav, at den dataansvarlige er stand til at redegøre for de særlige omstændigheder, som ligger til grund for den forsinkede anmeldelse.

De 72 timer gælder fra det tidspunkt, hvor den dataansvarlige bliver bekendt med databruddet. Hvis den dataansvarlige blot har en formodning om, at der er sket et brud på persondatasikkerheden, anses dette ikke som tilstrækkelig grund til at sætte de 72 timer i gang.

En forsinkelse af en anmeldelse kan i visse tilfælde forsvares. Dette gælder blandt andet, hvis den dataansvarlige har foretaget bestræbelser på at standse et brud, hvor der har været risiko for yderligere kompromittering af personoplysningerne. Det samme gælder, hvis den dataansvarlige er bekendt med, at personer, som er i besiddelse af personoplysningerne, har til hensigt at benytte oplysningerne til kriminelle formål, og den dataansvarlige i stedet har prioriteret at forhindre dette, fremfor at føre en rettidig anmeldelse.

Det er som udgangspunkt den dataansvarlige, der skal foretage anmeldelsen af et databrud til Datatilsynet. Den dataansvarlige kan, og bør i nogle tilfælde, udpege en eller flere medarbejdere, som får tilladelse til at anmelde brud på datasikkerheden til Datatilsynet på vegne af den dataansvarlige.

En databehandler vil også kunne anmelde brud på datasikkerheden til Datatilsynet, hvis denne har fået bemyndigelse til dette, såfremt at denne bemyndigelse er tydeliggjort i databehandleraftalen.

Det er dog altid den dataansvarlige, der har det primære juridiske ansvar for, at der sker anmeldelse til Datatilsynet, uanset om den dataansvarlige har bemyndiget andre til at kunne foretage anmeldelse eller ej.

Databehandlerens rolle ved et sikkerhedsbrud:

Sker et brud på persondatasikkerheden, er det databehandlerens ansvar at meddele den dataansvarlige herom. Databehandleren skal under alle omstændigheder informere om et sådant brud. Dette skal ske uden unødig forsinkelse, og der eksisterer derfor ikke en tydelig og klar tidsfrist for underretningen. Databehandlerens pligt til at informere den dataansvarlige i tilfælde af et databrud kan med fordel inddrages i databehandleraftalen.

Anmeldelsens indhold:

Når der anmeldes et brud på datasikkerheden, skal anmeldelsen som minimum indeholde:

* En beskrivelse af karakteren af bruddet – herunder kategorierne, antal berørte registrerede, antallet af berørte personoplysninger
* Navn og kontaktoplysninger på databeskyttelsesrådgiveren - eller andre relevante kontaktoplysninger
* En beskrivelse af de sandsynlige konsekvenser som følge af bruddet på persondatasikkerheden
* En beskrivelse af de foranstaltninger, som er truffet eller som foreslås truffet af den dataansvarlige som et led i indsatsen mod at afhjælpe bruddet.

Ovenstående er minimumskrav, og det forventes, at den dataansvarlige giver så mange oplysninger om bruddet som muligt i anmeldelsen.

**Underretning til den registrerede:**

Udover anmeldelse til Datatilsynet, har den dataansvarlige samtidig pligt til at meddele den/de registrerede, som kan eller vil blive påvirket af bruddet. Dette skal dog kun ske, hvis bruddet vurderes at indebære en ”høj risiko” for de registreredes rettigheder og frihedsrettigheder.

Formålet med denne underretning er at give den registrerede mulighed for at foretage foranstaltninger i tilfælde af, at der er sket eller vil ske kompromittering af den pågældendes personoplysninger.

I forordningen er der ikke nogen definition af, hvad ”høj risiko” indebærer. Dog gælder det, at en vurdering (som tidligere omtalt vedrørende anmeldelse til Datatilsynet) af risikoens omfang, skal lægges til grund. Jo mere alvorlige konsekvenser et brud kan medføre, jo større vil risikoen for de registreredes rettigheder og frihedsrettigheder være. Ligeledes vil en større sandsynlighed for, at bruddet vil få konsekvenser, være forbundet med en større risiko.

Det må bemærkes, at hvis det vurderes, at der foreligger en høj risiko for de registreredes rettigheder eller frihedsrettigheder, har det ikke nogen betydning hvor stort et antal af registrerede, der skal ske underretning til.

Underretningen til de registrerede skal ske uden unødig forsinkelse, efter at bruddet på persondatasikkerheden er blevet påvist, således at de registrerede kan foretage nødvendige foranstaltninger. Det bør bemærkes, at underretningen til de registrerede ikke er betinget af tidspunktet for, hvornår der er sket anmeldelse af databruddet til Datatilsynet.

Underretningen skal beskrive selve bruddet af datasikkerheden, og den skal som minimum indeholde nedenstående:

* Navn og kontaktoplysninger på databeskyttelsesrådgiveren, hvis virksomheden/organisationen har en sådan. Hvis ikke, så skal et andet kontaktpunkt angives, hvor den registrerede kan hente yderligere oplysninger om bruddet
* En beskrivelse af de sandsynlige konsekvenser, som bruddet på datasikkerheden kan have haft eller vurderes at kunne få
* En beskrivelse af de foranstaltninger, som den dataansvarlige allerede har truffet eller har tiltænkt at træffe, for at håndtere bruddet. Hvis det er relevant skal foranstaltninger, for at begrænse bruddets mulige skadevirkninger, angives.

Den dataansvarlige kan vælge at give den registrerede yderligere oplysninger om bruddet. Det vigtigste er, at underretningen fremstår klar og tydelig og er letforståelig.

Hvis det er muligt, og forekommer relevant, bør den dataansvarlige give den registrerede vejledning i, hvorledes den registrerede bedst kan beskytte sig mod mulige negative konsekvenser af bruddet.

Hvis ikke der sker en underretning til den/de registrerede, så kan Datatilsynet gå ind og kræve, at den dataansvarlige underretter den/de registrerede.

Underretningen til den/de registrerede skal ske direkte. Det vil sige, at det ikke er tilstrækkeligt f.eks. at udsende en pressemeddelelse, eller videresende et opslag på virksomhedens hjemmeside eller lignende. Direkte underrettelse kan f.eks. ske via e-mail, på sms, via brev eller lignende. Det gælder hertil, at underretningen ikke må sendes til den registrerede sammen med anden information. Det skal være klart og tydeligt for den registrerede, at vedkommendes personoplysninger har været udsat for et databrud.

Ansvaret for underretningen ligger også her hos den dataansvarlige. Den dataansvarlige vil dog kunne uddelegere opgaven til en databehandler eller en tredjemand. Det er under alle omstændigheder den dataansvarliges forpligtigelse, at en underretning sker rettidigt og korrekt.