S

Databrudspolitik
i Luthersk Mission

Juni 2024

Denne politik har til hensigt at beskrive retningslinjer for håndtering af brud på persondatasikkerheden. Den er ikke fyldestgørende men en kort gennemgang af Datatilsynets vejledning omkring emnet. Hele Datatilsynets vejledning kan læses her:
https://www.datatilsynet.dk/Media/637886298435856391/H%c3%a5ndtering%20af%20brud%20p%c3%a5%20persondatasikkerheden.pdf

Hvad er et brud på persondatasikkerheden?

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

Eksempler på databrud kan fx være:

- Hvis uautoriserede personer får adgang til personoplysninger. Det kan ske, hvis man kommer til at videregive personoplysninger til nogen, som ikke skulle have haft dem. F.eks. ved at sende en mail forkert, eller hvis man har personoplysningerne liggende et sted, hvor uautoriserede personer har adgang.
- Hvis computere bliver hacket. Det kan ske hvis it-systemer ikke er tilstrækkeligt sikrede, eller hvis kodeord eller adgange bliver misbrugt.
- Hvis man kommer til at slette eller ændre personoplysninger, som ikke skulle have været ændret og ikke kan genskabe det tabte igen.
- Hvis den nødvendige kryptering ikke bruges, kan følsomme personoplysninger blive kompromitteret.

Anmeldelse til Datatilsynet

Hvis det er sandsynligt, at et brud på personsikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal den dataansvarlige anmelde bruddet.

Man anmelder et brud på persondatasikkerheden via Virk.dk, der finder man en "Indberetning af brud på sikkerhed", det er en elektronisk blanket, som skal udfyldes af den dataansvarlige.

Brud på persondatasikkerheden skal anmeldes til Datatilsynet uden unødig forsinkelse og om muligt senest 72 timer, efter den dataansvarlige er blevet bekendt med bruddet. Hvis ikke anmeldelsen sker inden for 72 timer, skal den ledsages med en begrundelse for forsinkelsen.

En forsinkelse kan ske, hvis der er tale om et alvorligt brud på personsikkerheden, som endnu ikke er standset, og hvis der er fortsat risiko for yderligere kompromittering af personoplysninger, i sådanne tilfælde vil en dataansvarlig kunne retfærdiggøre en vis forsinkelse, som følge af dennes bestræbelse på at forhindre yderligere kompromittering.

Hvis den dataansvarlige ikke er i stand til at give alle nødvendige oplysninger til Datatilsynet inden for tidsfristen på de 72 timer, må den dataansvarlige give oplysningerne løbende. Man må *ikke* vente med at anmelde det for dermed at kunne give Datatilsynet en samlet melding. Det kan tage tid af afdække alle nødvendige oplysninger.

Når der sker et databrud, bør man vurdere:

- Typen af brud, er det tab af oplysninger, brud på fortroligheden eller integritetskrænkelse;

- Oplysningernes art og omfang;
- Risikoen for, at registrerede kan identificeres;
- Konsekvenserne for den registrerede. Er oplysningerne endt i hænderne på kriminelle personer eller til en person, den dataansvarlige har stor tillid til?
- Om bruddet involverer børn eller særligt udsatte personer;
- Antallet af berørte personer.

Det er ikke alle brud, som skal indberettes til Datatilsynet.

Hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, skal der ikke ske anmeldelse.

Eksempler på databrud, som ikke skal anmeldes:

- En person får stjålet sin taske, hvori der ligger en harddisk med følsomme personoplysninger. Harddisken er beskyttet med en stærk kryptering, der ikke umiddelbart vil være mulig for uvedkommende at dekryptere.
- En medarbejder kommer til at sende en mail med personoplysninger til en forkert mailmodtager, denne mailmodtager er en, medarbejderen kender godt og stoler på. Medarbejderen beder ham om at slette den sendte mail, medarbejderen kan efterfølgende stole på, at mailen bliver slettet.
- En medarbejder kommer til at uploade en fil på hjemmesiden, som indeholder flere CPR-numre. Medarbejderen opdager det straks og fjerner filen med det samme. Man kan efterfølgende konstatere ved hjemmesidens logoplysninger, at der ikke har været besøgende på hjemmesiden i den korte tid, hvor filen har været tilgængelig.

Underretning af den registrerede.

Hvis et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal der ikke kun foretages en anmeldelse til Datatilsynet, den registrerede skal også underrettes. Det skal ske hurtigst muligt og uden unødig forsinkelse.

Den registrerede får dermed mulighed for at træffe de nødvendige forholdsregler, det kan være at ændre sine logins, lukke sin bankkonto, eller hvad der er nødvendigt.
En underretning til en registreret skal om muligt indeholde en vejledning til, hvad vedkommende bør gøre for at mindske skaderne og en vejledning om, hvilke følgevirkninger, dette brud evt. kan få. Underretningen skal også beskrive de foranstaltninger, der er truffet for at håndtere bruddet.

Den registrerede skal underrettes direkte, via mail, brev, telefonopkald eller lign. En pressemeddelelse, eller via et nyhedsbrev er ikke tilstrækkeligt. Det afhænger selvfølgelig af situationen, har man mistet hele sit adressekartotek, kan man ikke skrive til folk direkte.

Intern dokumentation

Den dataansvarlige skal dokumentere alle brud på persondatasikkerheden, det er 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.

Der er ikke specifikke formkrav til dokumentationen, men den skal indeholde alle væsentlige beslutninger, der er truffet som følge af bruddet, som:

- 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?

Procedure for håndtering af databrud i Luthersk Mission

Når der sker et databrud i Luthersk Mission, skal der foretages en intern anmeldelse til sekretariatet. Der er i den forbindelse udarbejdet en vejledning (P3a Vejledning ifm. databrud i hele LM) til LM's medarbejdere og lokale samarbejdspartnere samt et skema (P3b Skema til udfyldelse ved databrud hos Luthersk Mission).

Alle medarbejdere og lokale samarbejdspartnere vil blive orienteret om pligten til at anmelde databrud og vil få adgang til relevante dokumenter herunder vejledning og indberetningsskema via SharePoint.

I vejledningen er der en nærmere beskrivelse og eksempler på, hvilke sikkerhedshændelser skal anmeldes til sekretariatet samt en række spørgsmål, der bør overvejes inden anmeldelse. Den interne anmeldelse sker ved at udfylde ovennævnte skema og sende det til sekretariatet pr. mail til dlm@dlm.dk. Anmeldelsen skal ske uden hurtigst muligt.

Sekretariatets GDPR-udvalg er ansvarligt for at vurdere ud fra indsendte skema og i samråd med den, der har indberettet bruddet, om der skal foretages anmeldelse til Datatilsynet, samt om de registrerede skal orienteres.

Når et brud på persondatasikkerheden sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, skal den enkelte registrerede underrettes hurtigst muligt.

Det er ikke nødvendigt at underrette den registrerede, hvis en af følgende betingelser er opfyldt:

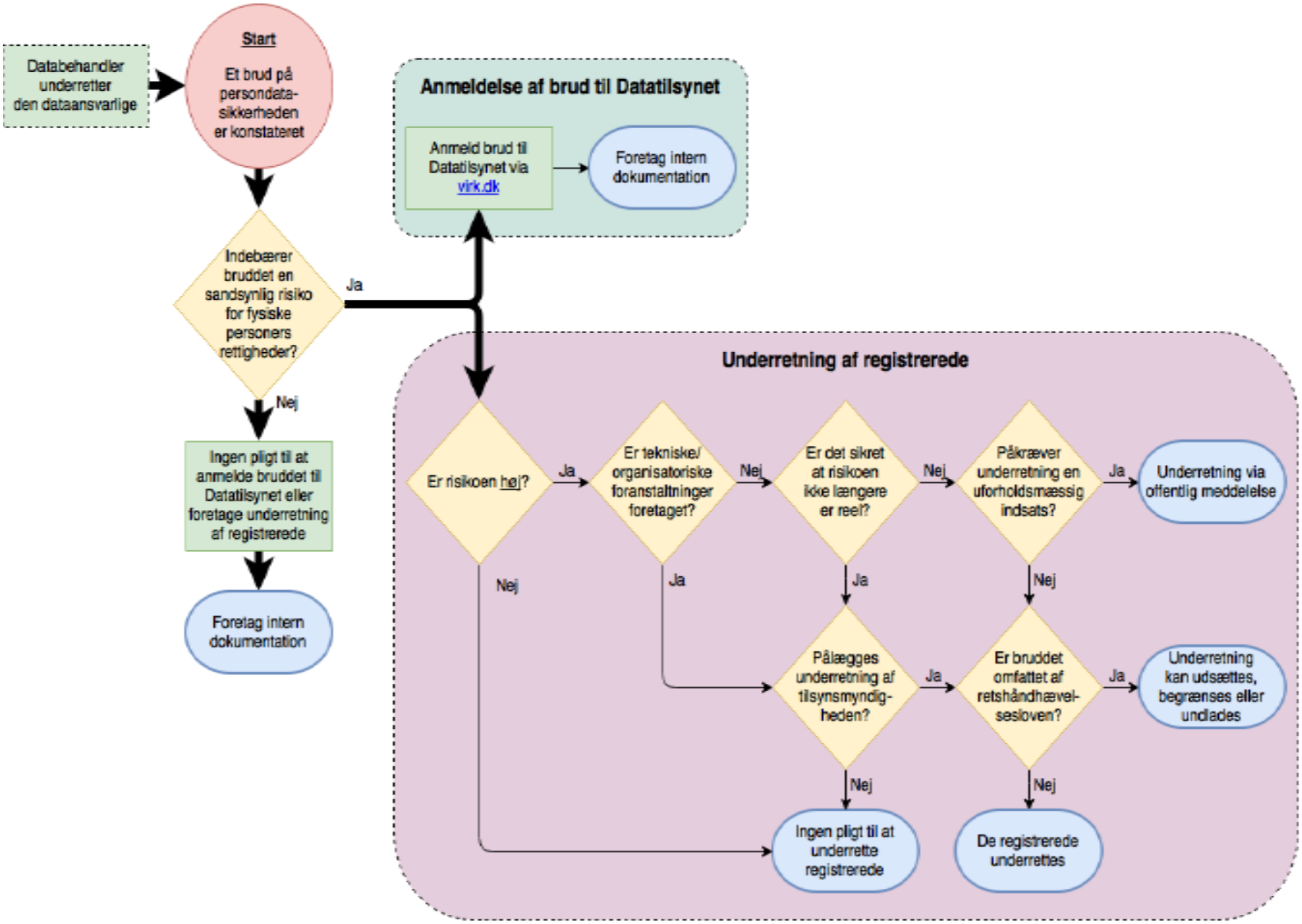
- Den dataansvarlige har gennemført passende tekniske og organisatoriske beskyttelsesforanstaltninger.
- Den dataansvarlige har truffet efterfølgende foranstaltninger, der sikrer, at den høje risiko for de registrerede ikke længere er reel.
- Det vil kræve en uforholdsmæssig indsats – i så fald skal der i stedet foretages en offentlig meddelelse eller tilsvarende foranstaltning, hvorved de registrerede underrettes på en tilsvarende effektiv måde.

Luthersk Mission vil 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. Anmeldelse til Datatilsynet vil ske trinvist, hvis det ikke er muligt at indberette samlet inden 72 timer.

Luthersk Mission vil opbevare dokumentation for alle databrud, herunder de faktiske omstændigheder, konsekvenser og trufne afhjælpende foranstaltninger også i de tilfælde, hvor det vurderes, at bruddet ikke skal anmeldes.

Processen er illustreret i nedenstående figur.

Procesbeskrivelse af, hvordan en sikkerhedshændelse håndteres i Luthersk Mission



Risikoprofil

Forhold, der taler for høj følsomhed ift. persondata:

- LM er en kirkelig organisation og betegnes dermed ift. Persondataforordningen (GDPR) som en religiøs organisation. Dermed er alle oplysninger, der kan identificere en person til LM, af personfølsom karakter.
- Tro og værdier, som de praktiseres i LM, kan fremkalde stærke modreaktioner hos modstandere. Vi oplever det yderst sjældent i Danmark, men det er et fokuspunkt i nogle arbejdslande. I Danmark vurderes den største risiko at være negativ omtale på diverse medieplatforme.
- Især sekretariatet ligger inde med personfølsomme data af forskellig beskaffenhed, der skal behandles.

Retningslinjer for, hvem der har adgang til persondata

En lang række nødvendige persondata er af en sådan karakter, at det kun er udvalgte nøglepersoner, som må have kendskab til dem. Det kan f.eks. være materiale i forbindelse med gavebreve, rekrutteringsforløb, sjælesørgeriske samtaler o. lign. Her benytter vi kun udvalgte medarbejdere, som ved ansættelse underskriver en ansættelseskontrakt, hvor de tilkendegiver, at de er bevidste om deres tavshedspligt og ansvar.

Retningslinjer for fysiske arkiver og dokumenter

På sekretariatet er det et fysisk arkiv i kælderen og ved musikkontoret, der bruges til LM's overordnede arkivering. Opbevaring af dokumenter i arkivet sker i henhold til "LM's politik for opbevaring og sletning af personoplysninger". Kun autoriserede personer har adgang til arkivet, og nøgler til arkivet opbevares af Resurseteamet.

Særligt vigtige dokumenter (skøder, gavebreve, stamkort, ansættelseskontrakter osv.) opbevares i et pengeskab på resursekontoret. Nøglen til skabet opbevares af Resurseteamet.