Dansk persondataret

Bent Ole Gram Mortensen (red.)

Dansk persondataret

Ex Tuto
PUBLISHING
www.extuto.com

Bent Ole Gram Mortensen (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Markvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Starup, Jøren Ullits & Frederik Waage
Dansk persondataret
Første udgave, første oplag

Denne bog er udgivet i januar 2020 af Ex Tuto Publishing A/S. Grafisk tilrettelæggelse og sats af mere.info A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis František Štorm i 2000 og Robert Slimbach i 1996. Jan Trzaskowski har stået for forlagsredaktion og Tove Møgelvang-Hansen har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m^2 af Narayana Press, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af Buchbinderei S.R. Büge GmbH i Celle. Bogen er fagfællebedømt.

Ex Tuto A/S er medlem af Forening for Boghaandværk, og vi støtter bæredygtig skovforvaltning ved at anvende FSC-certificeret papir.

Printed in Denmark 2020
ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S
Toldbodgade 55, 1.
DK-1253 København K
www.extuto.com

MIX
Papir fra ansvarlige kilder
FSC® C010651
www.fsc.org

Udgivet med støtte fra
dreyersfond

FairPublishing

Kapiteloversigt

Kapitel 14

Sikkerhed og håndtering af databrud

Daniel Hartfield-Traun

> "The so-called *risk-based approach* is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Article 17) and the DPA prior checking obligations (Article 20)."[1]

14.1. Baggrund

Sikkerhed i forbindelse med databeskyttelse er gammel vin på nye flasker. Der er med andre ord intet nyt i forhold til det risikobaserede arbejde, som organisationen skal udføre, når den søger at træffe passende tekniske og organisatoriske foranstaltninger i overensstemmelse med databeskyttelsesforordningen.[2]

Den risikobaserede fremgangsmåde gjorde sig også gældende under sikkerhedsbekendtgørelsen,[3] persondataloven[4] og databeskyttel-

1. Artikel 29-Gruppen WP 218, s. 2, 4. afsnit.
2. Artikel 5, stk. 1, litra f); artikel 24, stk. 1; artikel 25 og artikel 32.
3. Sikkerhedsbekendtgørelsen, § 3, stk. 1.
4. Persondatalovens § 41, stk. 3.

sesdirektivet.[5] Den eneste forskel er, at hvor det i dag hedder sig, at de tekniske og organisatoriske foranstaltninger skal være passende, skulle de førhen være fornødne. En sproglig ændring, der udover at understrege det forhold, at sikkerhedsniveauet skal være afstemt, ikke påvirker retstilstanden.[6] Forpligtelsen vedrører desuden såvel organisatoriske som tekniske foranstaltninger, hvilket vil sige, at alt fra arbejdsgange til it-system er omfattet.

14.2. Informationssikkerhed og databeskyttelse

Det er vigtigt at kende forskel på databeskyttelse og informationssikkerhed, da organisationen ellers vil nå det forkerte resultat. Informationssikkerhed defineres kort og godt som opretholdelse af informations fortrolighed, integritet og tilgængelighed.[7] Information kan i udgangspunktet være oplysninger om både ting og mennesker. Det kan siges, at alle personoplysninger er information, men ikke al information er personoplysninger.[8]

Information anses rent informationssikkerhedsmæssigt for at være et aktiv, der er nødvendigt for organisationens virke og drift, hvorfor den skal beskyttes.[9] Informationssikkerhed handler med andre ord grundlæggende om at beskytte organisationen ved at beskytte kritisk information, som har betydning for organisationen og dens drift. Et element vil i den sammenhæng bl.a. være at beskytte organisationens omdømme og økonomi mod bøder og offentlig påtale, der kunne følge i kølvandet på en lovovertrædelse.

Selvom overholdelse af lovregler og andre regulativer ganske vist er en inkorporeret del af informationssikkerhedsarbejdet,[10] er det i praksis de færreste virksomheder, der har taget højde for persondatareglerne i den relation.

5. Direktiv 95/46/EF.
6. Artikel 29-Gruppen WP 218, s. 3, nr. 4, fodnote 1.
7. ISO27001:2016, s. 6, nr. 2.33.
8. Databeskyttelsesforordningen, artikel 4, nr. 1.
9. ISO27001:2016, s. 15, pkt. 3.2.2.
10. ISO27001:2017, note til punkt 4.2 Understanding the needs and expectations of interested parties & Annex A punkt A.18.1.4 Privacy and protection of personally identifiable information-

Hvor informationssikkerhed handler om at beskytte organisationer, handler databeskyttelse om at beskytte fysiske personer. Beskyttelsen relaterer sig til behandling af personoplysninger, men der skal i den sammenhæng også tages hensyn til den frie udveksling af selvsamme personoplysninger.[11]

Det fokus, der er på de registrerede, er med andre ord grundlæggende i forbindelse med arbejdet med databeskyttelse. Det betyder samtidig, at en organisations arbejde med informationssikkerhed næppe vil kunne substituere arbejdet med databeskyttelse, da der sjældent har været fokus på både de registreredes og organisationens behov.

Arbejdet med at opretholde fortrolighed, integritet og tilgængelighed gør sig dog også gældende for persondataretten.[12] De metoder, der anvendes i den sammenhæng, herunder etablering af kontekst, risikovurdering og implementering af kontroller, er ligeledes ens for både databeskyttelse og informationssikkerhed. Den grundlæggende forskel er, om der er fokus på individ eller organisation.

14.3. Databeskyttelse i praksis – et overblik

Databeskyttelsesforordningen stiller krav om, at dataansvarlige såvel som databehandlere træffer passende tekniske og organisatoriske foranstaltninger.[13] Kravet rummer alle aspekter af behandling af personoplysninger, herunder hvordan organisationerne tilrettelægger manuelle arbejdsgange og indretter it-systemer.[14]

Det overordnende formål med foranstaltningerne er at sikre og gøre organisationen i stand til at påvise, at behandlingen er i overensstemmelse med databeskyttelsesforordningen.[15] Det medfører, at foranstaltningerne skal sikre effektiv implementering af databeskyttelsesprincipperne, integrering af de fornødne garantier i behandlingen for at opfylde kravene i databeskyttelsesforordningen og naturligvis

11. Databeskyttelsesforordningen, artikel 1, stk. 1.
12. Databeskyttelsesforordningen, artikel 32, stk. 1, litra b.
13. Databeskyttelsesforordningen, artikel 32, stk. 1 & præambelbetragtning (83), 1. pkt.
14. EDPB 2019, punkt 9.
15. Databeskyttelsesforordningen, artikel 5, stk. 2 & 24, stk. 1.

beskytte de registreredes rettigheder.[16] Implementeringsarbejdet skal blandt andet ske under hensyntagen til implementeringsomkostningerne.[17]

Der skal endvidere tages hensyn til konteksten, herunder behandlingens formål, karakter, omfang, sammenhæng,[18] og hvilken type personoplysninger der indgår i behandlingen.[19] Har organisationen ikke etableret sin kontekst, vil det svare til, at en læge stiller sin diagnose uden forudgående undersøgelse af patienten. Kuren er ikke altid to Panodil, og passende foranstaltninger er ikke altid kryptering.

Organisationen kan med fordel lægge kræfter i etablering af konteksten, da det kan have betydelig økonomisk og sikkerhedsmæssig indvirkning på organisationen og dennes overholdelse af databeskyttelsesretten. Organisationen skal i forbindelse med sin implementering også tage hensyn til de risici, af varierende sandsynlighed og alvor, for fysiske personers rettigheder og frihedsrettigheder, der er forbundet med behandlingsaktiviteterne.[20]

De enkelte risici kan eksempelvis udspringe af uautoriseret videregivelse af eller adgang til personoplysninger, fejlagtig eller ulovlig tilintetgørelse samt tab eller ændring af de personoplysninger, der behandles.[21]

Konsekvenserne for de registrerede kan være både fysiske, materielle eller immaterielle, især hvis behandlingen kan give anledning til skade på omdømme, finansielle tab, forskelsbehandling, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, identitetstyveri eller -svig eller uautoriseret ophævelse af pseudonymisering.[22] Andre betydelige økonomiske eller sociale konsekvenser vil også være relevante, hvis det kan resultere i, at de registrerede bliver berøvet deres

16. EDPB 2019, punkt 7.
17. EDPB 2019, punkt 23 og 24.
18. Databeskyttelsesforordningen, artikel 24, stk. 1, 25, stk. 1, 32, stk. 1 og præambelbetragtning (74), sidste pkt.
19. Databeskyttelsesforordningen, præambelbetragtning (51), 1. pkt.
20. Databeskyttelsesforordningen, artikel 24, stk. 1, artikel 25, stk. 1, artikel 32, stk. 1, præambelbetragtning (51), stk. 1 & (83), 3. pkt.
21. Databeskyttelsesforordningen, artikel 32, stk. 2.
22. Databeskyttelsesforordningen, præambelbetragtning (75).

rettigheder og frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger.[23]

Selve vurderingen af risici, herefter benævnt risikovurderingen, skal foretages på et objektivt grundlag, som giver mulighed for at fastslå, hvilken risiko behandlingsaktiviteten indebærer.[24] Under hensyntagen til de registreredes rettigheder, behandlingsaktiviteten og dens kontekst skal risikovurderingen tage højde for de konsekvenser, der er forbundet med behandlingsaktiviteten og sandsynligheden for, at de bliver aktuelle.[25]

Først når organisationens kontekst er etableret, og der er gennemført en grundig risikovurdering, kan organisationen reelt træffe beslutning om, hvilke tekniske og organisatoriske foranstaltninger det vil være passende at træffe. Lovgiver henviser selv til en række foranstaltninger, der kan træffes af både teknisk og organisatorisk karakter, herunder eksempelvis databeskyttelsespolitikker,[26] pseudonymisering[27] og kryptering.[28] EDPB har desuden i november 2019 publiceret materiale om det praktiske arbejde med data protection by design & default, hvori der blandt andet henvises til CNIL's online vejledning i design af aps og hjemmesider.[29]

Identificerer organisationen behandlingsaktiviteter, der indebærer høj risiko, er den forpligtet til at gennemføre en konsekvensanalyse vedrørende databeskyttelse forud for behandlingen (se nærmere herom i kapitel 12).[30] Uanset om det er tilfældet, er der ikke nogen udløbsdato på forpligtelsen til at træffe passende tekniske og organisatoriske foranstaltninger.[31] Organisationen er derfor til enhver tid forpligtet til at have truffet passende foranstaltninger. Det vil i øvrigt altid være en fordel og i visse tilfælde en forpligtelse at kunne påvise dette.[32] Forpligtelsen indebærer, at organisationen løbende skal ajourføre sin kontekst

23. Databeskyttelsesforordningen, præambelbetragtning (75).
24. Databeskyttelsesforordningen, præambelbetragtning (76), 2. pkt.
25. Databeskyttelsesforordningen, præambelbetragtning (76), 1. pkt.
26. Databeskyttelsesforordningen, artikel 24, stk. 2.
27. Databeskyttelsesforordningen, artikel 25, stk. 1.
28. Databeskyttelsesforordningen, artikel 32, stk. 1, litra a.
29. EDPB 2019, side 14, note 18.
30. Databeskyttelsesforordningen, artikel 35, stk. 1. Se nærmere herom i kapitel 12.
31. Databeskyttelsesforordningen, artikel 32, stk. 1.

og foretage nye risikovurderinger for at fastholde et passende databeskyttelsesniveau. En proces der efter lovgivers mening særligt skal tages stilling til.[33]

Det er desuden et krav, at organisationen er i stand til både at opdage og håndtere et brud på persondatasikkerheden.[34] Der er ikke mange organisationer, som kan slippe afsted med at lade stå til, hvis personoplysningernes fortrolighed, integritet eller tilgængelighed kompromitteres. Lovgiver mener derfor også, at genoprettelse af tilgængelighed kræver særlig stillingtagen.[35]

Udover at være forpligtet til internt at dokumentere alle brud på persondatasikkerheden,[36] vil organisationen i visse tilfælde også skulle anmelde bruddet til tilsynsmyndigheden.[37] Anmeldelse til Datatilsynet er et krav, medmindre det er usandsynligt, at bruddet indebærer en risiko for de registrerede.[38]

Det er desuden et krav, at anmeldelsen almindeligvis sker inden for 72 timer, efter at organisationen er blevet bekendt med bruddet. Det kræver i udgangspunktet en risikovurdering, før organisationen kan tage stilling til bruddets sandsynlige konsekvenser for de registrerede. Der skal derfor på baggrund af bruddets faktiske omstændigheder som minimum tages stilling til, om det sandsynligvis vil medføre skade på omdømme, finansielle tab, forskelsbehandling, tab af fortrolighed for personoplysninger, der er omfattet af tavshedspligt, identitetstyveri eller -svig, uautoriseret ophævelse af pseudonymisering eller andre betydelige økonomiske eller sociale konsekvenser.[39]

Viser det sig, at det ikke er usandsynligt, at bruddet medfører risici for de registrerede, skal organisationen som nævnt anmelde bruddet til Datatilsynet. Hvis det imidlertid viser sig, at bruddet vil indebære høj risiko for de registrerede, er organisationen forpligtet til også at under-

32. Databeskyttelsesforordningen, artikel 5, stk. 1, litra f), jf. artikel 5, stk. 2 & 28, stk. 3, 1. afsnit, litra h.
33. Databeskyttelsesforordningen, artikel 32, stk. 1, litra d.
34. Artikel 29-Gruppen WP 250 rev.01, sidste afsnit før punkt 3.
35. Databeskyttelsesforordningen, artikel 32, stk. 1, litra c.
36. Databeskyttelsesforordningen, artikel 33, stk. 5.
37. Databeskyttelsesforordningen, artikel 33, stk. 1.
38. Databeskyttelsesforordningen, artikel 33, stk. 1.
39. Databeskyttelsesforordningen, præambelbetragtning (85), 1. pkt.

rette de registrerede.[40] Organisationen kan dog helt slippe for at underrette de registrerede, hvis de berørte oplysningers fortrolighed bevares, fordi de eksempelvis er krypterede.[41]

Alternativt kan organisationen undsige sig underretningspligten, hvis den på bagkant af bruddet har sikret, at den høje risiko ikke længere er reel.[42] Derudover kan organisationer, der oplever massive brud på persondatasikkerheden, undtages pligten til at underrette de registrerede enkeltvis. Organisationen vil i stedet være forpligtet til at underrette de registrerede via en offentlig meddelelse, der har samme effekt som direkte underretning.[43] Endelig kan Datatilsynet, på baggrund af en risikovurdering, beslutte, om organisationen skal underrette de registrerede eller ej.[44]

14.4. Databeskyttelse i praksis – Bit by bit

I det følgende vil den risikobaserede tilgang blive beskrevet skridt for skidt. Processen er i hovedsagen den samme, uanset om der er tale om informationssikkerhed eller databeskyttelse. Der er dog visse undtagelser, som adresseres løbende.

14.4.1. Ledelsesforankring

Arbejdet med databeskyttelse og informationssikkerhed er for langt de fleste organisationer nyt. Det medfører derfor ofte en række ændringer i den daglige drift, hvorfor ledelsesforankring er et helt grundlæggende kriterie for at få succes med arbejdet. Sandsynligheden for succes minimeres med andre ord, hvis arbejdet ikke forankres i den øverste ledelse, men parkeres hos it-afdelingen eller den nye databeskyttelsesrådgiver (DPO), privacy manager eller tilsvarende. Først når ansvaret for efterlevelse er placeret i den øverste ledelse, kan organisationen reelt siges at have påbegyndt sikkerhedsarbejdet. Det skyldes, at de strategiske beslutninger, der senere skal træffes i forhold til, hvilket sikkerhedsniveau organisationen vil sigte efter, skal træffes af topledelsen. Ukendskab til

40. Databeskyttelsesforordningen, artikel 34, stk. 1.
41. Databeskyttelsesforordningen, artikel 34, stk. 3, litra a.
42. Databeskyttelsesforordningen, artikel 34, stk. 3, litra b.
43. Databeskyttelsesforordningen, artikel 34, stk. 3, litra c.
44. Databeskyttelsesforordningen, artikel 34, stk. 4.

loven er som bekendt ikke nogen undskyldning for ikke at efterleve den, og der foreligger ligeledes et arbejdsgiveransvar.[45] Når det overordnede ansvar for efterlevelse af persondataretten er placeret, kan de udførende kræfter gå i gang med det praktiske arbejde.

14.4.2. Etablering af kontekst

Det praktiske arbejde med informationssikkerhed såvel som databeskyttelse tager udgangspunkt i en kortlægning og forståelse af den pågældende organisations kontekst.[46] Organisationens kontekst skal etableres med udgangspunkt i organisationens mål med efterlevelse af persondataretten. Det giver i den sammenhæng bedst mening, at der tages udgangspunkt i organisationens behandlingsaktiviteter.

De fleste organisationer vil med fordel kunne tage udgangspunkt i deres lovpligtige fortegnelser.[47] Det skal dog understreges, at hvis organisationens fortegnelser alene imødekommer de juridiske minimumskrav som eksempelvis Datatilsynets bilag 6.1 i Vejledning om fortegnelser, vil der være behov for at supplere med yderligere information for at tegne et brugbart billede af organisationens kontekst.

Der er blandt andet behov for at anføre, hvilke aktiver der understøtter behandlingsaktiviteten. De understøttende aktiver er typisk lokalitet, hardware, software, netværk, personale m.v. I den relation kan der være hjælp at hente i internationalt anerkendte standarder.[48]

Derudover vil det være en fordel, hvis organisationen har dannet sig et overblik over, hvilke gængse sikkerhedspolitikker og -kontroller der allerede er etableret. Organisationen kan her tage udgangspunkt i de mest almindelige sikkerhedsprocedurer på plads[49] og -kontroller.[50]

---

45. DL 3-19-2.
46. Databeskyttelsesforordningen, betragtning (76).
47. Databeskyttelsesforordningen, artikel 30.
48. ISO27005:2011, afsnit 7 Context establishment; ISO27005:2011 Annex B, ISO31000:2009; ISO27001:2013, afsnit 4 Context of the organization; ENISA 2017a, s. 10, afsnit 2.1.1, Step 1: Definition of the processing operation and its context; ENISA 2016, afsnit 3.1, Step 1: defining the processing operation and its context.
49. Center for Internet Security 2019.
50. ISO27001:2013, Annex A og ISO27002:2013, afsnit 5-18.

14.4.2.1. Sårbarhedsvurdering

En del af optegningen af organisationens kontekst er sårbarhedsvurderingen. Organisationen skal her identificere sine sårbarheder med henblik på at tage stilling til, hvorvidt og hvordan de skal adresseres.

En sårbarhed er udtryk for en svaghed, som kan medføre, at en trussel aktualiseres, hvis den udnyttes.[51] Svagheden kan indfinde sig i processer, systemer eller mangel på samme.

Manglende aflåsning af døren til HR-chefens arkivskabe er et eksempel på en sårbarhed. Udnyttelse af sårbarheden kan medføre, at personoplysninger i arkivskabene kommer til uvedkommendes kendskab.

Organisationen kan med fordel tage udgangspunkt i etablerede internationale standarder,[52] når den skal identificere sine sårbarheder.

Persondataretten handler om beskyttelse af de registrerede. Organisationen er derfor også nødt til at tage stilling til, om den skal og i givet fald kan imødekomme forordningens krav om håndtering af de registreredes rettigheder. Det vil sige, at organisationen skal vurdere, om der er sårbarheder relateret til håndtering af oplysningspligten,[53] indsigtsretten[54] og retten til dataportabilitet[55] med videre.

En persondataretlig sårbarhed kunne være manglende procedurer for identitetssikring i forbindelse med håndtering af indsigtsretten. Udnyttelse af denne sårbarhed kunne medføre, at personoplysninger kom til uvedkommendes kendskab.

Resultaterne bliver forarbejdet til optegning af de hændelsesscenarier, der senere skal underlægges en risikovurdering.

Organisationen kan også foretage tekniske sårbarhedsskanninger af sine systemer. Det anbefales helt generelt, at organisationen vælger veletablerede og velrenommerede udbydere, da der ofte er forøget risiko forbundet med anvendelse af freeware.[56]

---

51. ISO27000: 2016, punkt 2.89.
52. ISO27005:2011, Annex D.
53. Databeskyttelsesforordningen, artikel 13 og 14.
54. Databeskyttelsesforordningen, artikel 15.
55. Databeskyttelsesforordningen, artikel 20.
56. Freeware er software, som ikke kræver monetærbetaling.

Når organisationen har identificeret sine sårbarheder, skal det vurderes, hvorvidt de kan udnyttes og dermed er relevante at arbejde videre med.

Tilstedeværelsen af en sårbarhed er ikke i sig selv skadevoldende. Skaden opstår først, når sårbarheden påvirkes af en trussel. Organisationen skal derfor tage stilling til, om der er trusler, som kan påvirke de identificerede trusler.

Identificerer organisationen en sårbarhed, som ikke påvirkes af nogle trusler, bør den pågældende sårbarhed noteres og løbende overvåges i tilfælde af, at situationen ændrer sig.

14.4.3. Trusler

Organisationen skal med udgangspunkt i sin kontekst, herunder de implementerede sikkerhedsforanstaltninger og identificerede sårbarheder, tage stilling til, hvilke trusler der er relevante.

En trussel defineres informationssikkerhedsmæssigt som en potentiel kilde til en hændelse, som kan resultere i skade på organisationen.[57] Persondataretligt vil der være tale om en potentiel kilde til ulovlig behandling eller et decideret brud på persondatasikkerheden. Det vil sige, at organisationen skal identificere og efterfølgende gennemgå truslerne for at spørge sig selv, om truslen med udgangspunkt i organisationens kontekst kan påvirke en sårbarhed med det resultat, at der sker ulovlig behandling eller et brud på persondatasikkerheden.

Truslerne kan overordnet inddeles således, at nogle udspringer af miljø i bred forstand, herunder vind og vejr, men også indendørsklima. Andre trusler kræver, at et menneske begår fejl, eller at en person aktivt søger at udnytte en sårbarhed.

Der findes indtil flere trusselskataloger med velbeskrevne trusler af både generel[58] og specifik[59] karakter. Katalogerne kan dog ikke stå alene, og der vil oftest være behov for at supplere dem med trusler, som

57. ISO27001:2017, afsnit 2.83.
58. Bundesamt für Sicherheit in der Informationstechnik; ISO27005:2011, Annex C, Examples of typica threats.
59. ISO29134:2017, Annex B, Generic threats; ENISA 2017a, afsnit 3.3, Step 3: Definition of possible threats and evaluation of their likelihood.

er unikke for organisationen. Hér kan organisationen eventuelt tage udgangspunkt i tidligere hændelser.

Det er vigtigt at huske på, at behandlingsaktiviteten i sig selv kan udgøre en trussel – det handler med andre ord ikke kun om hackere og sure medarbejdere.

Lovgiver har i forordningen anført tre behandlingsaktiviteter, hvis gennemførsel i sig selv medfører, at der skal tages særlige databeskyttelsesmæssige hensyn.[60] Det drejer sig blandt andet om profilering, der ligger til grund for afgørelser,[61] men også overførsel af personoplysninger til tredjelande eller internationale organisationer.[62]

Her adskiller informationssikkerhed sig markant fra databeskyttelse. En informationssikkerhedsmæssig risikovurdering tager udgangspunkt i, hvilke konsekvenser en trussel kan have for organisationens evne til at indfri sine mål, hvad enten det er at øge indtjeningen, yde service til borgerne eller nødhjælp til ofrene for en naturkatastrofe. Den databeskyttelsesretlige konsekvensvurdering tager derimod udgangspunkt i de registrerede, herunder deres rettigheder og frihedsrettigheder, uanset om der er tale om organisationens egne ansatte, kunder eller hjemmesidebesøgende.

Uanset om organisationen kan koble en trussel til en sårbarhed eller ej, bør organisationen nedskrive sine begrundelser for vurderingen. Kobles truslen til en sårbarhed, bør de allerede skitserede hændelsesscenarier uddybes.

En persondataretlig sårbarhed kunne være manglende procedurer for identitetssikring i forbindelse med håndtering af indsigtsretten. Udnyttelse af denne sårbarhed kunne medføre, at personoplysninger kom til uvedkommendes kendskab. Sårbarheden kunne udnyttes af enhver, som med vilje eller ved en fejl opgav en andens navn for derved at få fat i oplysninger om vedkommende.

Optegning af konkrete hændelsesscenarier er en forudsætning for gennemførelse af risikovurderingen.

---

60. Databeskyttelsesforordningen, artikel 35, stk. 3.
61. Databeskyttelsesforordningen, artikel 35, stk. 3, litra a.
62. Databeskyttelsesforordningen, kapitel V, Overførsel af personoplysninger til tredjelande og internationale organistioner.

14.4.3.1. Trusselsaktører

En trusselsaktør er en person, som kan realisere en trussel ved at udnytte en sårbarhed med det resultat, at den realiserede trussel får konsekvenser for de registrerede. Helt overordnet kan trusselsaktører inddeles i fire kategorier:

Den første er interne aktører, der handler uagtsomt eksempelvis en medarbejder, der fejlagtigt aktiverer ransomware[63] f.eks. via en phishing-mail[64].

I 2015 forsøgte medarbejdere hos Nordfyns kommune og Gribskov kommune at åbne vedhæftede filer med det resultat, at de kom til at installere ransomeware, som krypterede kommunernes respektive data.[65]

Den næste er interne aktører, som handler forsætligt. Forsætligt udførte handlinger er udtryk for, at vedkommende med vilje overtræder reglerne. Det kan eksempelvis være en fortørnet medarbejder, som misbruger sin adgang til personoplysninger.

I perioden fra maj 2008 frem til 2012 solgte en ansat ved Nets' underleverandør IBM oplysninger om 135 kendtes brug af kreditkort til Se og Hør, med en fortjeneste på mindst 430.000 kr.[66]

Den tredje kategori er eksterne uagtsomme aktører. Det kan eksempelvis være leverandører, konsulenter og andre besøgende, der bringer deres egne maskiner ind i organisationen og på den måde inficerer organisationens maskiner eller netværk, fordi de ikke ved, at deres eget udstyr er inficeret.

De amerikanske told- og grænsemyndigheder (U.S. Customs and Border Protection) oplevede i 2019, at en databehandler blev angrebet af hacker-gruppe Team Snatch. Angrebet lykkedes, fordi databehandleren ikke havde truffet de sikkerhedsforanstaltninger, der var fastsat i

63. Ransomware er software, der krypterer systemer og filer, hvorefter organisationen eller personen kan tilbagekøbe adgang hos angriberen.
64. En phishing-mail er en e-mail, der sendes med henblik på at narre modtager til at handle på en bestemt måde, som for eksempel at installere ransomware.
65. Wind 2015.
66. Berlingske 2016.

aftalen.[67] Resultatet var, at kørekortoplysninger om godt 100.000 personer blev sat til salg på dark web[68].

En sidste kategori er eksterne aktører, der handler forsætligt. Det kan være personer, der har et horn i siden på organisationen, og som derfor gerne vil orkestrere et læk af personoplysninger.

37 millioner brugere af dating sitet for gifte, Ashley Maddison, fik i 2015 offentliggjort deres personoplysninger. Offentliggørelsen skete som resultat af et motiveret hack angiveligt gennemført af gruppen "The Impact Team".[69]

14.4.3.2. M-M-O

Forkortelsen er udtryk for motive, means og oppurtunity, som oversættes til motiv, kompetencer og muligheder. Der er her tale om de elementer, der almindeligvis inddrages, når det skal vurderes, om det er relevant at tage højde for en bestemt trusselsaktør i forbindelse med et bestemt hændelsesscenarie.

Vurderingen går ud på, at organisationen først vurderer, hvorvidt og i hvilket omfang en identificeret trusselsaktør er motiveret til at realisere en given trussel med henblik på at kompromittere personoplysningernes fortrolighed, integritet eller tilgængelighed. Motiverne kan være mange, eksempelvis økonomi, generel utilfredshed eller status.

Når organisationen har vurderet trusselsaktørens motiv, vurderes trusselsaktørens kompetenceniveau i forhold til den pågældende trussel. Det kan eksempelvis være tekniske kompetencer, hvis der er tale om en trussel af teknisk karakter.

Endelig tager organisationen stilling til, hvad trusselsaktørens muligheder er for at realisere den pågældende trussel. Eksempelvis har interne aktører ofte bedre mulighed for at realisere trusler mod organisationens arbejdsgange end eksterne aktører.

---

67. Kirk 2019.
68. "The Dark Web er ikke en fagterm som sådan, men et udtryk der bruges om en del af internettet, hvor al kommunikation kan foregå fuldstændig anonymt." – se Villumsen & Moestrup 2017.
69. Hackett 2015.

14.4.4. Risikovurdering

Hele vurderingen af, hvorvidt de foranstaltninger, organisation har truffet, er "passende", står og falder med risikovurderingen.[70] Risikovurderingen består helt grundlæggende af en række på hinanden følgende vurderinger af de konsekvenser, der kan være forbundet med en behandlingsaktivitet, og sandsynligheden for, at de aktualiseres.

Der findes indtil flere forskellige standarder for gennemførelse af risikovurderinger, som organisationen kan gøre brug af.[71] Valget er i og for sig frit, så længe fokus er på de registrerede og deres rettigheder.

Uanset hvad, er grundelementerne i en risikovurdering konsekvens og sandsynlighed.

14.4.4.1. Konsekvensvurdering

Organisationen skal starte med at beslutte, hvilke kriterier der skal være udslagsgivende for konsekvensvurderingen. Databeskyttelsesretligt har lovgiver allerede indiceret, hvilke kriterier der skal lægges til grund, herunder fysisk, materiel og immateriel skade.[72]

Helt konkret nævnes blandt andet skade på omdømme, forskelsbehandling og andre betydelige eller økonomiske konsekvenser, hvis de registrerede kan blive berøvet deres rettigheder eller frihedsrettigheder eller forhindret i at udøve kontrol med deres personoplysninger.[73] Det er i den relation vigtigt at inddrage de registreredes muligheder for at gøre deres databeskyttelsesretlige rettigheder[74] gældende, eksempelvis retten til indsigt,[75] dataportabilitet[76] og indsigelse mod automatiske individuelle afgørelser, herunder profilering[77] i det omfang, de er relevante.

70. EDPB 2019, afsnit 2.1.1.
71. ISO27005:2011; ISO29134:2017; NIST 2012.
72. Databeskyttelsesforordningen, betragtning (75).
73. Databeskyttelsesforordningen, betragtning (75).
74. Databeskyttelsesforordningen, kapitel III, Den registreredes rettigheder.
75. Databeskyttelsesforordningen, artikel 15.
76. Databeskyttelsesforordningen, artikel 20.
77. Databeskyttelsesforordningen, artikel 22.

Konsekvensvurderingen skal ikke udelukkende være skadesbetinget, og der bør derfor også tages stilling til samfundsmæssige konsekvenser, herunder generel tillid til e-handel og lignende.[78]

Det anbefales, at vurderingen nedfældes og i øvrigt gøres både kvalitativ og kvantitativ.

Det vil sige, at organisationen bør søge både at angive konsekvensen som en talværdi, helst på en skala bestående af et lige antal, f.eks. fra 1 til 4. Anvendelsen af skala med et lige antal sikrer, at organisationen kan bruge alle vurderinger og ikke ender med en lunken mellemvurdering f.eks. 3 på en skala fra 1-5, som efterfølgende skal revurderes.

Den kvalitative vurdering sikrer organisationens mulighed for at styre og spore de enkelte vurderinger. Helt konkret bør nummerering suppleres af en kort og præcis beskrivelse af de bagvedliggende overvejelser.

14.4.4.2. Sandsynlighedsvurdering

Sandsynlighedsvurderingen er det andet ben i den samlede risikovurdering, og organisationens kontekst er altafgørende for sandsynlighedsvurderingen. Under hensyntagen til alle identificerede og relevante objektive forhold tager organisationen stilling til, hvor sandsynligt det er, at en trussel realiseres med det resultat, at det får konsekvenser for de registrerede. Det anbefales, at sandsynlighedsvurderingen også foretages både kvantitativt og kvalitativt.

14.4.5. Risiko

Risiko er udtryk for kombinationen af konsekvens og sandsynlighed. Når organisationen har foretaget både konsekvensvurdering og sandsynlighedsvurdering af de relevante trusselsscenarier, kan risikoen fastlægges for hver af disse.

Ledelsen skal desuden tage stilling til, om den gennemførte risikovurdering er tilfredsstillende.[79] I modsat fald skal den tilpasses og gennemføres på ny.

Har organisationen valgt at forholde sig kvantitativt til konsekvens og sandsynlighed, vil det være muligt at sammenlægge eller

78. Artikel 29-Gruppen WP 218, s. 4, nr. 11.

79. ISO27005: 2011, punkt 9.1, figur 3.

gange de anførte værdier med hinanden. Resultatet vil være den risiko, der er forbundet med trusselsscenariet.

Resultatet kan anføres i en matrix, som angivet nedenfor:

4	gul	gul	rød	rød
3	gul	gul	gul	rød
2	grøn	gul	gul	gul
1	grøn	grøn	gul	gul
Sandsynlighed / konsekvens	**1**	**2**	**3**	**4**

Figur 14.1. Risikoprofil. "Farverne" i matricen kan også bruges til at udtrykke organisationens risikoappetit.

14.4.6. Risikoappetit

Risikoappetitten er udtryk for, hvor risikovillig organisationen er i relation til en bestemt behandlingsaktivitet. Det er topledelsens opgave at fastslå organisationens risikoappetit.

Det er i den relation vigtigt at tage højde for de registreredes, lovgivers og tilsynsmyndighedernes forventede risikoappetit. Sammenholdt med organisationens egen risikoappetit vil organisationen kunne fastlægge, hvornår der skal reageres på en given trussel. Organisationen vil hurtigt opdage, at tilsynsmyndighederne, lovgiver, de registrerede og organisationen selv vil acceptere forskellige niveauer af risici.

Kerneeksemplet er oplysninger om fagforeningsmæssigt tilhørsforhold. Behandling af denne type oplysninger har lovgiver bestemt, kun undtagelsesvis må finde sted.[80] Det standpunkt vil tilsynsmyndighederne være forpligtet til at følge, selvom mange danskere ikke kerer sig synderligt om, hvem der ved, at de er medlem af en bestemt fagforening. Organisationen kan derfor lade sig friste til at acceptere relativt høje risici i forbindelse med behandlingen af disse oplysninger, hvis

80. Databeskyttelsesforordningen, artikel 9.

kun de registreredes risikoappetit tages til indtægt. Det kan imidlertid vise sig at være uhensigtsmæssigt, hvis uheldet er ude, og tilsynsmyndighederne ønsker at efterse organisationens risikovurdering.

Farveangivelsen (her i gråtoner) i risikomatricen ovenfor er standard, og organisationen kan derfor give udtryk for sin risikoappetit ved en farveforskydning.

Det kan eksempelvis være tilfældet i sundhedssektoren, hvor markeringen er gul i rubrikkerne, hvor konsekvensen er 4 og sandsynligheden er 1 og 2. Her kunne der være et ønske om to røde markeringer med henblik på at afspejle organisationens risikoappetit og for at sikre hurtig og effektiv risikohåndtering.

4	gul	gul	rød	rød
3	gul	gul	gul	rød
2	grøn	gul	gul	rød
1	grøn	grøn	gul	rød
Sandsynlighed / konsekvens	**1**	**2**	**3**	**4**

Figur 14.2. Justeret risikoprofil.

14.5. Risikohåndtering

Ledelsen skal på baggrund af risikovurderingen tage stilling til, hvorvidt og i givet fald hvordan de enkelte risici nedbringes til et acceptabelt niveau. Da der allerede er taget stilling til organisationens generelle risikoappetit, kan der med fordel tages udgangspunkt i denne.

Håndtering af risici kan almindeligvis munde ud i flere handlinger. Helt overordnet kan disse inddeles i, at risikoen accepteres, nedbringes, deles eller helt undgås.

14.5.1. Risikodeling

Når to eller flere organisationer fordeler risikoen ved gennemførelse af en proces mellem sig, er der tale om risikodeling. Det kan eksempelvis være en organisation og dennes leverandør, som deler den risiko, der er forbundet med levering af en vare eller ydelse til en kunde. Databeskyttelsesretligt forholder det sig dog således, at det i udgangspunktet ikke er muligt at dele risici. Det skyldes, at de angivne risici vedrører de registrerede og ikke organisationen. Det er derfor ikke muligt at sprede risikoen ud på flere registrerede, da det umiddelbart vil være i strid med formålet med databeskyttelsesreglerne. Det vil i øvrigt hverken nedbringe konsekvenserne for en registreret eller sandsynligheden for et brud, at andre registrerede udsættes for samme risiko.

14.5.2. Risikoeliminering

Organisationen har også mulighed for helt at eliminere risikoen ved at afstå fra at gennemføre behandlingsaktiviteten.

Det kan vise sig at være nødvendigt, når en organisation forud for iværksættelse af en behandlingsaktivitet gennemfører en risikovurdering, som viser, at der er høj risiko forbundet med aktiviteten. Ønsker organisationen ikke at arbejde på at nedbringe den høje risiko, vil det mest naturlige være helt at afstå fra at iværksætte behandlingen.

14.5.3. Risikonedbringelse

I de fleste tilfælde vil der være tale om behandlingsaktiviteter, som er nødvendige for organisationens drift og udvikling. Derfor vælger mange organisationer at sætte sig for at nedbringe de risici, der er forbundet med deres behandlingsaktiviteter. Informationssikkerhedsmæssigt kan organisationen arbejde på at nedbringe både konsekvens og sandsynlighed.

Det skyldes, at konsekvenserne relaterer sig til organisationen selv, og den er derfor i stand til eksempelvis at gøre sig mindre afhængig af den pågældende proces ved hjælp af redundans. Dette er dog ikke tilfældet rent databeskyttelsesretligt. Konsekvenserne for de registrerede ligger almindeligvis uden for organisationens indflydelsessfære.

Organisationen kan eksempelvis ikke ændre på, hvilke konsekvenser det har for de registrerede, at oplysninger om en disciplinærsag

offentliggøres. Det betyder samtidig, at konsekvenserne for de registrerede ikke er organisationsspecifikke, da de ikke relaterer sig til disse. Det er med andre ord underordnet for konsekvensen for de registrerede, hvorvidt offentliggørelsen af eksempelvis betalingskortoplysninger lækkes af en webshop, en bank eller den registrerede selv.

Det vil dog fortsat være relevant at tage højde for kulturelle forskelle på tværs af sektorer, regioner og landegrænser. Behandling af personoplysninger anskues eksempelvis forskelligt i Danmark og Tyskland.

Uanset om organisationen arbejder med informationssikkerhed eller databeskyttelse, vil den kunne påvirke sandsynligheden i større eller mindre grad. Databeskyttelsesretligt bør fokus være på at minimere sandsynligheden for, at en trussel aktualiseres.

14.5.4. Risikoaccept

Organisationen kan også vælge at acceptere den risiko, der er forbundet med behandlingsaktiviteten. Det er her vigtigt at huske på, at organisationen accepterer risikoen på vegne af de registrerede, da de sjældent har mulighed for at give deres besyv med. Høring af de registrerede er dog et krav i visse tilfælde, når der udarbejdes en konsekvensanalyse vedrørende databeskyttelse.[81] Organisationer, der har udpeget en databeskyttelsesrådgiver, er ligeledes forpligtet til at inddrage denne.[82]

14.5.5. Implementeringsrammer

Vælger organisationen at nedbringe risikoen, er der i udgangspunktet ganske få begrænsninger. Én af disse fremgår direkte af forordningen: at organisationens skal tage højde for implementeringsomkostningerne.[83] Dette hensyn skal lægges til grund, hvad enten der er tale om tekniske eller organisatoriske foranstaltninger.[84]

En anden begrænsning må udledes af principperne for behandling af personoplysninger, herunder princippet om lovlighed, rimelig-

81. Databeskyttelsesforordningen, artikel 35, stk. 9.
82. Databeskyttelsesforordningen, artikel 38, stk. 1.
83. Databeskyttelsesforordningen, artikel 25 & 32.
84. EDPB 2019, punkt 23 og 24.

hed og gennemsigtighed samt princippet om formålsbegrænsning. Denne begrænsning består i, at organisationen i implementeringen af sikkerhedsforanstaltninger skal sørge for, at foranstaltningerne i sig selv ikke ender med at krænke de registreredes rettigheder. Det kan eksempelvis være tilfældet i henhold til netværksovervågning, hvor organisationen i større eller mindre grad logger, hvad medarbejderne sender og modtager.

Udover ovennævnte skal ledelsen på baggrund af organisationens kontekst tage stilling til, hvilke rammer der skal være i arbejdet med at nedbringe risici. Der kan både være tale om ressourcer i form af økonomi og mandetimer, men også kultur og påvirkning af organisationens muligheder for at indfri egne mål.

Organisationen er nu klar til på et oplyst grundlag at træffe passende tekniske og organisatoriske foranstaltninger.

Organisationen skal i den sammenhæng tage højde for, hvad det koster at implementere, hvad der teknisk er muligt, og de risici, der relaterer sig til organisationens behandlingsaktiviteter.[85]

14.5.6. Tekniske og organisatoriske foranstaltninger

Når organisationen har sat rammen, skal det besluttes, hvilke tekniske og organisatoriske foranstaltninger der skal træffes. Det er i den relation ikke et absolut krav, at foranstaltningerne både er tekniske og organisatoriske.

Eksempelvis kan organisationen kun indskærpe over for de ansatte, at de er omfattet af tavshedspligt, uden teknisk at kunne afskære dem fra at tale om tavshedspligtbelagte oplysninger.

Det anbefales dog, at teknikken understøtter interne forskrifter og procedurer, og at de ansatte tilsvarende oplæres i brugen af de tekniske løsninger, som organisationen indskærper, at de skal gøre brug af. Det kan eksempelvis være kryptering af hardware og e-mails.

Databeskyttelsesretligt udpeger lovgiver kryptering,[86] pseudonymisering[87] og den generelle evne til at opretholde fortrolighed, integri-

85. Databeskyttelsesforordningen, artikel 32, stk. 1, 1. afsnit, og EDPB, s. 26.
86. Databeskyttelsesforordningen, artikel 32, stk. 1, litra a.
87. Databeskyttelsesforordningen, artikel 25, stk. 1.

tet og tilgængelighed samt robusthed[88] af behandlingssystemer og -tjenester.[89] Lovgiver sætter også beredskab på dagsordenen, navnlig i forhold til personoplysningernes tilgængelighed.[90]

Endelig nævnes procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed[91] som tekniske og organisatoriske foranstaltninger, det kan være relevant at tage stilling til. De af lovgiver anførte foranstaltninger er af meget generel karakter og kan i realiteten komme til udtryk ved mange forskelligartede løsninger. Der findes indtil flere opgørelser over mere konkrete løsninger af organisatorisk såvel som teknisk karakter,[92] som organisationen kan tage udgangspunkt i.

14.5.6.1. Databeskyttelse gennem design og standardindstillinger

Databeskyttelsesretten er teknologineutral og har siden direktivet reguleret tilrettelæggelsen af et passende niveau for databeskyttelse ganske overordnet, både hvad angår sikkerhed og lovlighed.[93] Det vil sige, at forpligtelsen til at træffe passende tekniske og organisatoriske foranstaltninger altid har gjort sig gældende både for de organisationer, der køber færdigudviklet software, og den der bidrager til eller selv udvikler software.[94]

Databeskyttelsesforordningen stiller imidlertid skarpt på databeskyttelsesarbejdet med indførelsen af forpligtelserne i artikel 25, som regulerer databeskyttelse gennem design og standardindstillinger, navnlig i relation til udvikling af produkter og services[95]. Forpligtelsen

88. EDPB 2019, punkt 15.
89. Databeskyttelsesforordningen, artikel 32, stk. 1, litra b.
90. Databeskyttelsesforordningen, artikel 32, stk. 1, litra c.
91. Databeskyttelsesforordningen, artikel 32, stk. 1, litra d.
92. ISO27001:2003, Annex A; ISO27002:2017; ENISA 2017a, afsnit 5. Safety and security; ENISA 2016, afsnit 4, Security measures; NIST 2013, og EDPB 2019.
93. Direktiv 95/46/EF, artikel 17, stk. 1.
94. Artikel 29-Gruppen WP 29, Artikel 29-Gruppen WP 202, afsnit 3.1 Applicable law, 1. og 2. pkt.
95. Databeskyttelsesforordningen, præambelbetragtning (78), 3. pkt.

gælder dog for alle organisationer og kan eksempelvis komme til udtryk i disses interne politikker.[96]

I praksis er arbejdet med at finde frem til, hvad der er passende foranstaltninger, også det samme, uanset om organisationen stiler efter at imødekomme de specifikke eller generelle databeskyttelsesforpligtelser. Konteksten skal etableres, og der skal foretages risikovurderinger og implementeres passende foranstaltninger. I den forbindelse skal organisationen gøre sig de samme overvejelser.[97]

Hvad angår de foranstaltninger, der skal træffes, relaterer lovgiver ofte disse til principperne for behandling af personoplysninger[98] og henviser derfor specifikt til eksempelvis minimering af mængden af personoplysninger, der behandles, hurtig pseudonymisering og gennemsigtighed i behandlingen for de registrerede.[99] I praksis findes der en del materiale om foranstaltninger, som er udarbejdet med design og standardindstillinger for øje.[100] Der er på sin vis tale om en undergruppering af foranstaltninger, som almindeligvis kaldes "Privacy Enhancing Technologies" (PETs).

14.5.7. Restrisiko

Når organisationen har valgt, hvordan den vil gribe de identificerede risici an, vil den skulle foretage en ny risikovurdering, forudsat forholdene har ændret sig. Uanset hvordan organisationen vælger at gå til værks, vil den ende med en form for restrisiko.

Restrisiko er udtryk for resultatet af organisationens valg. Vælger organisationen at arbejde på at nedbringe risikoen, nedbringes den oprindelige risiko forhåbentligt med det resultat, at en ny risikovurdering vil vise en mindre restrisiko. På tilsvarende vis vil organisationens beslutning om at afstå fra at gennemføre behandlingsaktiviteten eller acceptere de forbundne risici medføre, at restrisikoen enten helt forsvinder eller forbliver uforandret.

96. Databeskyttelsesforordningen, præambelbetragtning nr. 78, 2. pkt.
97. Databeskyttelsesforordningen, præambelbetragtning nr. 78, 1. pkt.
98. Databeskyttelsesforordningen, artikel 5.
99. Databeskyttelsesforordningen, præambelbetragtning nr. 78, 3. pkt.
100. ENISA 2017; ISO29101:2018; ISO29191:2012, og EDPB 2019.

Det er som nævnt ikke muligt at dele risikoen, da den relaterer sig til enkeltindivider, og deres situation ikke bliver bedre af, at andres bliver værre.

Er resultatet, at organisationen identificerer behandlingsaktiviteter, som indebærer høj risiko for de registrerede, skal der gennemføres en konsekvensanalyse.[101] De eneste forskelle på risikovurderingen og konsekvensanalysen er, at der rent juridisk stilles minimumskrav til konsekvensanalysens anvendelse og form i artikel 35. Processen er i praksis den samme.

14.5.8. Opretholdelse og evaluering

Procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed[102] er en af de foranstaltninger, lovgiver sætter fokus på. Da der ikke er nogen udløbsdato på forpligtelsen til at træffe passende tekniske og organisatoriske foranstaltninger,[103] vil løbende evaluering og tilpasning være en forudsætning for, organisationens efterlevelse af forpligtelsen.[104]

14.6. Brud på persondatasikkerheden og anmeldelse

Før eller siden vil de fleste – hvis ikke alle – organisationer, opleve brud på persondatasikkerheden. I Danmark er der siden 25. maj 2018 og frem til 30. september 2019 foretaget 7.700 anmeldelser til Datatilsynet.[105] Anmeldelserne udspringer direkte af forordningen,[106] som stiller krav om, at brud på persondatasikkerheden anmeldes til tilsynsmyndigheden, "medmindre det er usandsynligt at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder". For at finde ud af, om et brud er anmeldelsespligtigt, er organisationen derfor nødt til at foretage en risikovurdering af det konkrete brud.

101. Databeskyttelsesforordningen, artikel 35, stk. 1
102. Databeskyttelsesforordningen, artikel 32, stk. 1, litra d.
103. Databeskyttelsesforordningen, artikel 32, stk. 1.
104. EDPB 2019, punkt 31.
105. Datatilsynet 2019, s. 9.
106. Databeskyttelsesforordningen, artikel 33, stk. 1.

14.6.1. Hændelsesoverblik

Organisationen er indledningsvist nødt til at etablere konteksten.[107]

Det vil i den sammenhæng være nærliggende at tage udgangspunkt i den information, der alligevel skal afgives, hvis det viser sig, at der skal ske anmeldelse til Datatilsynet.

Tid er en faktor i forbindelse med anmeldelse, da den om muligt skal ske, senest 72 timer efter organisationen er blevet bekendt med bruddet.[108]

14.6.2. Risikovurdering af brud på persondatasikkerheden

Når organisationen har fået overblik over hændelsen og sikret sig, at det er omfattet af definitionen af brud på persondatasikkerheden,[109] er næste skridt at foretage en risikovurdering.

Da bruddet allerede er sket, er det ikke relevant at vurdere, hvor sandsynligt det er, at det vil ske. Det er dog fortsat relevant at vurdere, hvilke umiddelbare konsekvenser der er forbundet med det pågældende brud. Derudover vil det være relevant at tage stilling til de afledte trusler, som bruddet kan give anledning til, herunder de forbundne konsekvenser og sandsynligheden for, at de indtræder.

14.6.3. Afhjælpende foranstaltninger

Organisationens næste opgave er at tage stilling til, hvilke foranstaltninger der kan afhjælpe bruddet, og træffe disse. Det vil i de fleste tilfælde være muligt for organisationen at begrænse skadesvirkningen af bruddet. Det kan eksempelvis ske ved, at organisationen retter henvendelse til en eventuel modtager af fejlagtigt afsendte personoplysninger og anmode vedkommende om at slette og bekræfte sletningen af disse. Hele processen dokumenteres både af hensyn til organisationens eget videre arbejde med forbedring af sikkerheden, og fordi det følger af forordningen.[110]

---

107. Databeskyttelsesforordningen, præambelbetragtning nr. 87, 1. pkt.
108. Databeskyttelsesforordningen, artikel 33, stk. 1.
109. Databeskyttelsesforordningen, artikel 4, nr. 12.
110. Databeskyttelsesforordningen, artikel 33, stk. 5.

14.6.4. Underretning af de registrerede

Dokumentationen kan i særdeleshed vise sig at være relevant i forhold til brud på persondatasikkerheden, som er vurderet til sandsynligvis at indebære høj risiko for de registrerede. Det skyldes, at denne type brud almindeligvis skal følges op af en underretning af de registrerede.[111] Der findes dog en række undtagelser fra dette udgangspunkt.[112]

Den første undtagelse består i, at organisationen har truffet passende foranstaltninger for at imødekomme bruddet, før det indfinder sig.[113] Lovgiver anfører som eksempel kryptering.[114] Det er vigtigt at understrege, at der alene er tale om et eksempel, og at kryptering ikke er den eneste måde at værne mod et brud på. Diskkryptering er dog en oplagt foranstaltning, da de mest udbredte styresystemer giver adgang til dette gratis.[115] Kryptering vil desuden minimere risikoen for, at personoplysningerne kommer til uvedkommendes kendskab.

En kommune, der eksempelvis får stjålet nogle bærbare PC'er, som er harddiskkrypterede, vil i udgangspunktet være omfattet af undtagelsen. Det skyldes, at harddiskkryptering gør det nær umuligt for uvedkommende at få adgang og kendskab til oplysningerne. Kommunen vil derfor umiddelbart være undtaget fra forpligtelsen til at underrette de registrerede.

Den anden undtagelse kan gøres gældende, hvis organisationen, efter bruddet har fundet sted, har truffet foranstaltninger, som sikrer, at den oprindeligt høje risiko, der var forbundet med bruddet, ikke længere er reel.[116] Oplever organisationen eksempelvis, at den mister en computer, tablet eller telefon, kan den søge at foretage remote wipe.[117] Remote wipe og kryptering kræver, som de fleste andre foranstaltnin-

111. Databeskyttelsesforordningen, artikel 34, stk. 1.
112. Databeskyttelsesforordningen, artikel 34, stk. 3.
113. Databeskyttelsesforordningen, artikel 34, stk. 3, litra a.
114. Databeskyttelsesforordningen, artikel 34, stk. 3, litra a.
115. Microsoft og iOS giver mulighed for gratis harddiskkryptering ved hjælp af henholdsvis BitLocker og FileVault.
116. Databeskyttelsesforordningen, artikel 34, stk. 3, litra b.
117. Remote wipe består i at organisationen fra centralt hold tager kontrol med det bortkomne materiale med henblik på at slettet alt indhold.

ger, at organisationen har gjort en forudgående indsats, herunder konfigureret enhederne korrekt.

Den sidste undtagelse fra direkte underretning af de registrerede kan gøres gældende, hvis organisationen vurderer, at det vil kræve en uforholdsmæssig indsats.[118] I sådanne tilfælde vil organisationen være forpligtet til at foretage en offentlig meddelelse, der har samme oplysende effekt som direkte underretning.[119]

Sendes ukrypterede CD'er med helbredsoplysninger om fem millioner personer eksempelvis til den forkerte modtager, er den dataansvarlige umiddelbart ikke forpligtet til at rette henvendelse til hver enkelt. I den situation vil det være mere nærliggende, at den dataansvarlige melder hændelsen ud til den brede offentlighed.

118. Databeskyttelsesforordningen, artikel 34, stk. 3, litra c, 1. pkt.
119. Databeskyttelsesforordningen, artikel 34, stk. 2, litra c, 2. pkt.