Vejledende tekst om risikovurdering

Datatilsynet og Rådet for Digital Sikkerhed

Juni 2019

Rådet for Digital Sikkerhed

DATATILSYNET

Indhold

Forord

Rådet for Digital Sikkerhed og Datatilsynet udgiver i samarbejde nogle praktisk orienterede hjælpetekster, som kan bidrage til, at især mindre dataansvarlige lettere kan få styr på nogle af de sikkerhedsorienterede forhold, der er relevante, når der behandles personoplysninger.

I denne første tekst adresseres det, hvordan den dataansvarlige kan gennemføre en risikovurdering i praksis.

1. Sikkerhed

Sikkerhed spiller en central rolle i databeskyttelsesforordningen: Sikkerhed er blevet ophøjet til at være et af de grundlæggende principper for behandling af personoplysninger. De sikkerhedsforanstaltninger, som skal iværksættes, skal vælges på baggrund af risikovurdering. Der er specifikke krav om anmeldelse og evt. underretning ved brud på persondatasikkerheden. Mere generelt er mange af tiltagene, der skal iværksættes i henhold til forordningens kapitel 4, en del af god sikkerhedspraksis og ISO2700X - f.eks. styring af leverandører (databehandlere), udpegelse af ansvarlige, brug af branchestandarder samt code of conducts m.v.

2. Risici

Som følge af at sikkerhed er blevet mere centralt placering i lovgivningen, er risici og vurdering af disse også blevet mere centralt placeret. Risici spiller en rolle i forhold til, hvilke foranstaltninger den dataansvarlige konkret skal iværksætte, se f.eks.:

- Artikel 24: risici er afgørende for hvilke foranstaltninger, der skal iværksættes
- artikel 25: risici er afgørende for hvilke designmæssige foranstaltninger, der skal iværksættes
- artikel 32: risici er afgørende for hvilke sikkerhedsforanstaltninger, der skal iværksættes
- artikel 33: risici er afgørende for, om der skal ske anmeldelse af brud på persondatasikkerheden til Datatilsynet
- artikel 34: risici er afgørende for, om den registrerede skal underrettes ved sikkerhedsbrud
- artikel 35: risici er afgørende for, om der skal gennemføres konsekvensanalyse
- artikel 36: risici er afgørende for, om Datatilsynet skal høres i forbindelse med en konsekvensvurdering
- artikel 39: databeskyttelsesrådgiverens anbefalinger skal bl.a. bero på en vurdering af risici.

Fordelen ved en risikobaseret tilgang til valg af sikkerhedsforanstaltninger er, at den dataansvarlige skal vælge netop de foranstaltninger, som er relevante ud fra risici – i stedet for at implementere foranstaltninger fra en eller anden lovbestemt liste, som måske eller måske ikke var dækkende for de reelle risici, der er relevante i den dataansvarliges kontekst. En risikobaseret tilgang skaber således en optimering af forbruget af ressourcer samtidig med at det skaber den røde tråd i sikkerheds- og dokumentationsarbejdet. Til gengæld stiller det også større krav til den dataansvarlige, som skal gøre sig i stand til at vurdere risici for den registrerede, når der behandles personoplysninger.

3. Risikovurdering set fra de registreredes perspektiv

De fleste organisationer har allerede lavet risikovurderinger for at kunne vælge og implementere de rette sikkerhedsforanstaltninger. Genstanden for disse risikovurderinger har imidlertid været organisationerne selv – altså hvad sker der med organisationens bundlinje eller gode ry og rygte, hvis den bliver hacket. Det er absolut nødvendigt at have lavet sådanne risikovurderinger – men det er ikke sådanne vurderinger databeskyttelsesforordningen lægger op til, at der skal laves.

Genstanden for databeskyttelsesforordningens risikovurderinger er de registreredes rettigheder og frihedsrettigheder. Der skal altså laves en vurdering af, hvilke risici organisationen som dataansvarlig udsætter kunder, medarbejdere og andre samarbejdspartnere i form af fysiske personer for.

Den dataansvarlige kan altså ikke genbruge sin risikovurdering, men er nødt til at lave en ny med de registrerede i centrum. Til gengæld kan den dataansvarlige genbruge sit risikovurderingsframework, fordi metodikken ved de to risikovurderinger er ens.

4. Risikovurderingsmetodik

Indledningsvist er det relevant at bemærke, at databeskyttelsesforordningen ikke siger noget om, hvor detaljeret risikovurderingen skal være. Den dataansvarlige må fastlægge et passende niveau henset de risici, som er relevante for den dataansvarliges behandling af personoplysninger.

Inden man går i gang med sin risikovurdering, skal man have et overblik over sine informationsaktiver. Informationsaktiverne kan være servere, it-systemer, kommunikationskanaler m.v., hvor der behandles personoplysninger. Hvert informationsaktiv bør have en ejer, som evt. også kan være risikoejer.

Når man arbejder med sikkerhed, skal man have de grundlæggende parametre fortrolighed, tilgængelighed og integritet på plads. Fortrolighed betyder, at informationer skal beskyttes mod uautoriseret adgang eller videregivelse, således at uvedkommende altså ikke kan gøre sig bekendt med oplysningerne (f.eks. beskyttelse mod hackere). Tilgængelighed betyder, at informationer skal beskyttes mod en uautoriseret adgangsbegrænsning for personer, som har retmæssig adgang (f.eks. nedbrud så systemer ikke er tilgængelige). Integritet betyder, at informationer skal beskyttes mod uautoriseret ændring eller ødelæggelse (f.eks. et systems pålidelighed og nøjagtighed til at udsende lønsedler).

Når man laver en risikovurdering, går man typisk frem trin for trin efter nedenstående metodik.

4.1 Konsekvensvurdering

For hvert informationsaktiv starter man med at fastlægge konsekvensen (høj, medium, lav) ved tab af aktivets fortrolighed, tilgængelighed og integritet. Der er som nævnt ikke krav til detaljeringsniveauet, så den dataansvarlige kan evt. gruppere sine informationsaktiver eller lave én samlet konsekvens for aktivet i stedet for at opdele på tilgængelighed, fortrolighed og integritet. Det er den dataansvarlige som træffer beslutning om detaljeringsgraden.

4.2 Trusselsvurdering

Herefter skal den dataansvarlige identificere de trusler, informationsaktiverne står overfor og vurdere, hvad sandsynligheden (høj, medium, lav) er, for at truslen bliver realiseret.

Hvis man ikke kender noget til trusler, f.eks. hacking, virus, phishing og ransomware, kan man lade sig inspirere af f.eks. ENISAs trusselskatalog, af OCTAVEs trusselsterminologi, af Soloves trusselstaxonomi eller af Center for Cybersikkerheds trusselsvurderinger.

Når man har identificeret sine trusler, kan det også være vanskeligt at sige noget om sandsynligheden for, at truslen manifesterer sig i en hændelse. Man bør for det første tillægge egne historiske data stor vægt – hvilke trusler har faktisk manifesteret sig i form af sikkerhedshændelser hos den dataansvarlige? Har den dataansvarlige været udsat for hacking, phishing eller ransomware, tyveri af personoplysninger, fejludsendelse af personoplysninger til forkert modtager eller har medarbejderne uploadet personoplysninger til private cloudtjenester. Man kan supplere sine historiske data med tendenser og statistikker fra nogle af de store antivirusproducenters årsrapporter.

Det er vigtigt at erkende, at fastlæggelse af trusler og konsekvenser ikke skal anskues som en videnskabelig disciplin. Den dataansvarlige må komme med sit bedste bud og stå ved det.

4.3 Sårbarhedsvurdering

Der er givetvis allerede iværksat sikkerhedsforanstaltninger, som har en mitigerende effekt i forhold til de trusler, som er identificeret under trusselsvurderingen. Eksisterende sikkerhedsforanstaltningerne skal sammen med deres bidrag til at reducere sandsynlighed og konsekvens kortlægges.

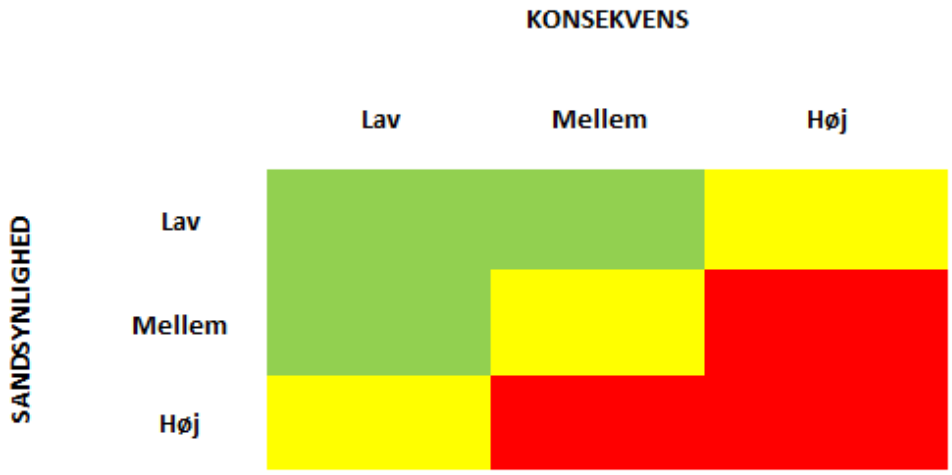
4.4 Risikobilledet

På baggrund af ovenstående kan man nu beskrive risikobilledet:

(konsekvensen x sandsynligheden) – eksisterende foranstaltninger = risikoen.

Ledelsen skal så tage stilling til, om risikoen er acceptabel, eller om der skal iværksættes ekstra foranstaltninger, som kan nedbringe risikoen yderligere. Ledelsen skal acceptere den restrisiko, som altid vil være tilbage.

Man kan sammenfatte ovenstående i nedenstående figur, hvor man især skal være opmærksom på, om nogle af informationsaktiverne eller personoplysninger er placeret i den røde del af figuren.



5. En gratis skabelon til risikovurdering

Erhvervsstyrelsen og Rådet for Digital Sikkerhed har lavet et risikovurderingsframework, som det er muligt at hente gratis online.

Når man bruger denne skabelon, tager man stilling til:

- Hvilke trusler kan påvirke fortrolighed, tilgængelighed eller integritet?
- Hvem ejer risikoen?
- Hvorfor er dette en risiko?
- Hvad er konsekvensen (på en skala fra 1-5) ved at en trussel materialiserer sig?
- Hvorfor er konsekvensen netop det?
- Hvad er sandsynligheden (på en skala fra 1-5) for at en trussel materialiserer sig?
- Hvorfor er sandsynligheden netop det?
- Herefter vejes risiko og sandsynlighed sammen til en beregnet risiko, som vil falde i en henholdsvis rød, gul og grøn kategori.
- Ledelsen kan vælge at acceptere, forsikre, overvåge eller undgå den identificerede risiko.
- Hvis ledelsen ønsker at undgå risikoen, så kan der iværksættes nye foranstaltninger af såvel teknisk som organisatorisk karakter.
- Herefter beregnes en ny konsekvens, sandsynlighed og restrisiko, som ledelsen så igen skal beslutte sin holdning til.

Det gode ved at bruge en fremgangsmåde som skitseret ovenfor er, at man på en struktureret måde får styr på alle argumenterne for de valg, man som dataansvarlig træffer. Dette kan bruges overfor eksterne interessenter og myndigheder, som kunne have interesse i at få indsigt i den dataansvarliges risikovurdering. Videre får man argumentationen på plads for valg af de foranstaltninger, som man bruger ressourcer på at implementere, når man skal rapportere til ledelsen om argumenter for brug af ressourcer og fremtidige ønsker til nye foranstaltninger. Endelig kan resultatet af ovenstående betragtes som en del af og grundlaget for den dataansvarliges arbejde med sikkerhedsstandarden ISO2700X. Risikovurderingen er således grundlaget for at skabe en rød tråd i både den dataansvarliges sikkerhedsarbejde og arbejde med at sikre overholdelse af databeskyttelsesreglerne.

Det skal for god ordens skyld bemærkes, at ovenstående blot er et eksempel på et af mange frameworks til at lave risikovurderinger.

6. Links

Datatilsynets vejledning om Behandlingssikkerhed og Databeskyttelse gennem design og standardindstillinger: https://www.datatilsynet.dk/media/6879/artikel25og32-vejledning.pdf.

Henning Mortensens artikel i R&R, nr. 5, 2018 om Behandlingssikkerhed – herunder risikovurdering: https://www.karnovgroup.dk/artikler/rr-05-2018-sikkerhedsforanstaltninger.

Risikovurderingsskabelon fra Erhvervsstyrelsen og Rådet for Digital Sikkerhed: https://sikkerdigital.dk/virksomhed/saadan-beskytter-du-din-virksomhed/skabeloner-og-vaerktoejer/.

ISO27005, Standard til at gennemføre risikovurderinger: https://webshop.ds.dk/da-dk/søgning/ds-iso-iec-270052018.

Soloves trusselstaxonomi: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf.

ENISAs trusselstaxonomi (især figuren, side 8): https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information.

OCTAVE (se især tabel 7, side 50): https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf.

Vejledende tekst om risikovurdering

Udgivet 21. juni 2019 af:
Datatilsynet
Borgergade 28, 5.
1300 København K
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk

Foto: Datatilsynet

Datatilsynet
Borgergade 28, 5.
1300 København K
T 33 19 32 00
dt@datatilsynet.dk
datatilsynet.dk