Organisatorisk og teknisk implementering af GDPR i Rigsarkivet

Fagligt forum
3. september 2019
Jan Dalsten Sørensen
Rigsarkivet

Indhold

1. Generelt om GDPR
2. Risikobaseret tilgang til informationssikkerhed
3. Tekniske og organisatoriske foranstaltninger

Synsvinklen er ”modtagelse, bevaring og tilgængeliggørelse af digitalt skabte arkivalier”

RIGSARKIVET

Generelt om GDPR

- Efterfølger til direktivet om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger (1995), som implementeret i persondataloven (2000)
- GDPR vedtaget 2016, trådte i kraft maj 2018

Personoplysninger

”En personoplysning er enhver form for information, der kan henføres til en bestemt person, også selv om personen kun kan identificeres, hvis oplysningen kombineres med andre oplysninger.”

Kilde: Datatilsynet

Typer af oplysninger

- Almindelige oplysninger
- Særlige kategorier af oplysninger (følsomme oplysninger)
- Oplysninger om straffedomme og lovovertrædelser eller tilknyttede sikkerhedsforanstaltninger

Særlige kategorier af oplysninger iht. artikel 9

- ”oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering”

Risikobaseret tilgang

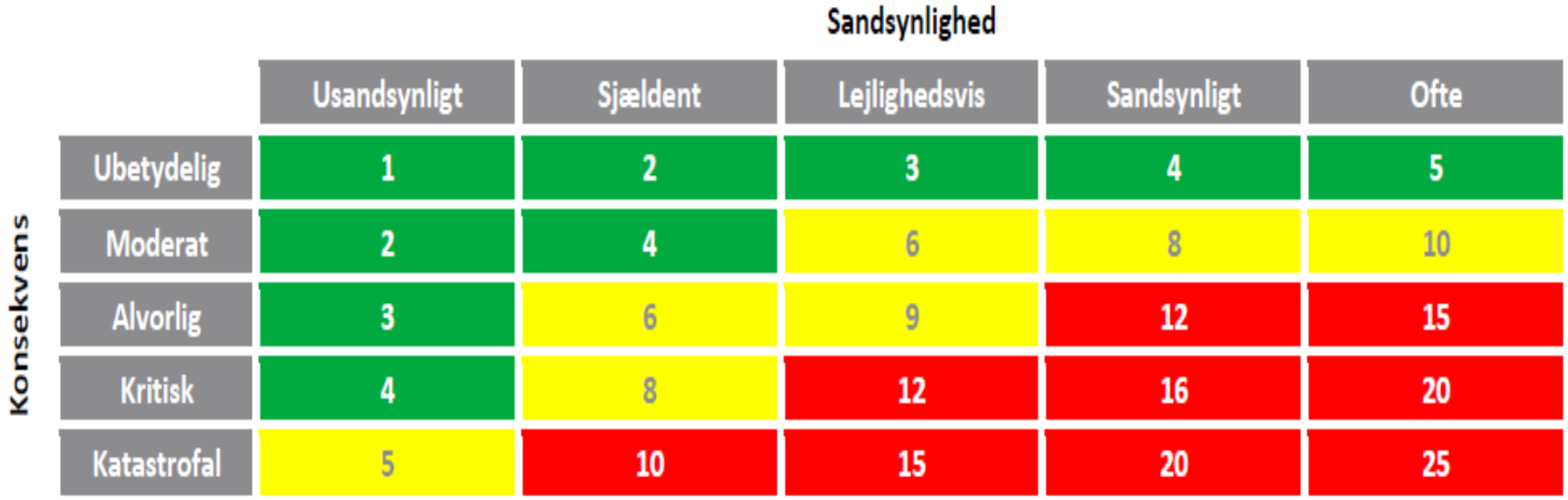
- Organisatoriske og tekniske foranstaltninger til sikring af personoplysningernes fortrolighed, tilgængelighed og integritet fastsættes ud fra en risikovurdering

Risikovurdering

- Risikoen for en trussel mod datas fortrolighed, tilgængelighed eller integritet vurderes ud fra sandsynlighed og konsekvens:
  - Hvor sandsynligt er det, at hændelsen/truslen indtræffer?
  - Hvor alvorlige er konsekvenserne, hvis hændelsen/truslen indtræffer?

RIGSARKIVET

Risikoniveauer



Konsekvens	Usandsynligt	Sjældent	Lejlighedsvis	Sandsynligt	Ofte
	Sandsynlighed				
Ubetydelig	1	2	3	4	5
Moderat	2	4	6	8	10
Alvorlig	3	6	9	12	15
Kritisk	4	8	12	16	20
Katastrofal	5	10	15	20	25

Konsekvensanalyse (DPIA)

”Hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder, foretager den dataansvarlige forud for behandlingen en analyse af de påtænkte behandlingsaktiviteters konsekvenser for beskyttelse af personoplysninger”

Tekniske og organisatoriske foranstaltninger

- Artikel 32 om behandlingssikkerhed, bl.a.
  - Pseudonymisering og kryptering af personoplysninger
  - Evne til at sikre vedvarende fortrolighed, tilgængelighed, integritet og robusthed af behandlingssystemer og -tjenester
  - Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en teknisk hændelse
  - En procedure for regelmæssig afprøvning og vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed

Fortegnelse (artikel 30)

- En fortegnelse skal bl.a. omfatte oplysninger om
  - Formålene med behandlingen
  - Beskrivelse af kategorier af registrerede og kategorier af personoplysninger
  - Kategorier af modtagere
  - Hvis muligt, de forventede tidsfrister for sletning

Design og standardindstillinger

- Forordningen kræver, at man i systemudvikling mm. arbejder med ”databeskyttelse gennem design” og ”databeskyttelse gennem standardindstillinger”

RIGSARKIVET

Spørgsmål?

E-post: jds@sa.dk
Twitter: jdalsten

Illustration: digitalbevaring.dk