Rådet for Digital Sikkerhed

12. juni 2019

Rådet for Digital Sikkerheds vejledning om GDPR

Det er vanskeligt for mange mindre organisationer at få greb om persondataforordningen i praksis. Både for så vidt angår det at komme i gang og for så vidt angår at fastholde fokus på området over tid. RfDS har derfor lavet denne korte vejledning, som har til formål at gøre arbejdet med GDPR mere operationelt – både når man skal til at starte op, og når man er godt i gang.

Baggrund

25. maj 2018 kom der nye regler for behandling af personoplysninger. Reglerne omfatter en række principper for behandling, som de dataansvarlige organisationer altid skal efterleve. Videre skal de sikre, at de personer, der behandles personoplysninger om, de registrerede, altid kan udleve deres rettigheder. Endelig skal de sikre, at de forpligtelser, der påhviler dem, også efterleves. Alle tiltag skal dokumenteres. Der er potentielt store bøder forbundet med ikke at efterleve reglerne.

Reglerne er vedtaget for at operationalisere retten til privatlivets fred, som er en fundamental rettighed fastsat i EU charter om grundlæggende rettigheder. Privatlivets fred er en grundlæggende rettighed, fordi det konstituerer det at være menneske, at man selv kan bestemme, hvilke personoplysninger man ønsker at dele med hvem hvornår. I praksis betyder denne ret som udgangspunkt, at man ikke behøver at være transparent i forhold til de oplysninger om f.eks. seksuelt, politisk eller religiøst tilhørsforhold, sundhedsmæssige forhold og økonomiske forhold – man har selv retten til at bestemme, hvem man deler disse oplysninger med. Det har mange steder i verden stor betydning, fordi f.eks. politiske minoriteter forfølges af magthaverne og seksuelle minoriteter forfølges af andre borgere. Tilsvarende har det i Europa også haft stor betydning, fordi politiske eller religiøse dissidenter er blevet forfulgt, og fordi kvinder historisk ikke har haft de samme rettigheder og muligheder som mænd. Privatlivets fred er således en vigtig værdi at værne om.

I gang med GDPR

Der er mange måder, at komme i gang med og lede et GDPR-projekt. Organisationerne skal gøre det på den måde, som passer bedst til deres organisationen. RfDS har dog erfaring for at det er en god ide at komme igennem nedenstående forhold:

1. **Ansvarsplacering**
   Ledelsen skal beslutte, hvem der skal stå i spidsen for de GDPR-tiltag, som skal iværksættes. Det er vigtigt at sikre at de fornødne tekniske og organisatoriske kompetencer er til rådighed. GDPR-projektlederen skal referere til ledelsen, således at ledelsen godkender alle beslutninger, som træffes. Projektlederen skal sikre at organisationen kommer igennem de øvrige trin.

2. **Indledende awareness**
   Ledelsen og medarbejderne skal bibringes forståelse om GDPR, således at de hver især forstår, hvad der forventes af dem for at GDPR-projektet kan komme i mål. Der kan med fordel identificeres privatlivsidealister i organisationen, som har en særlig forkærlighed for at beskytte personoplysninger. Disse personer kan med fordel trækkes ind i projektet og støtte projektlederen.

3. **Den juridiske to-do-liste**
   GDPR er et omfattende og komplekst regelsæt. Hertil kommer den danske implementering i form af Databeskyttelsesloven, retspraksis, EU-domme og udtalelser og afgørelser fra Det Europæiske Databeskyttelsesråd, m.v. Det er vigtigt at skabe sig et overblik over hvilke af alle disse regler, der er relevante for organisationen. Som udgangspunkt skal alle organisationer sikre, at de:
   a. Efterlever de grundlæggende principper, hvor de bl.a. skal fastslå formål med behandlingen af personoplysninger
   b. Fastslår på hvilket retligt grundlag, de behandler de forskellige oplysninger, f.eks. samtykke, kontrakt eller interesseafvejning
   c. Iværksætter tiltag, der sikrer, at de registrerede kan udleve deres rettigheder, f.eks. oplysning om behandlingerne, og retten til at få indsigt i data og få dem slettet
   d. Iværksætter foranstaltninger, som understøtter den dataansvarliges forpligtelser, f.eks. god sikkerhed, godt design af løsningerne og evt. udpegelse af en databeskyttelsesrådgiver
   e. Har identificeret det lovlige retlige grundlag, som evt. bruges til at overføre personoplysninger til tredjelande.

4. **Sammenhæng mellem GDPR og sikkerhed**
   Sikkerhed er centralt i GDPR, og en betydelig del af arbejdet er derfor at få implementeret en passende informationssikkerhed. Der skal laves en risikovurdering set fra de registreredes perspektiv ved, at organisationen behandler personoplysninger. På baggrund af denne risikovurdering skal der implementeres passende tekniske og organisatoriske foranstaltninger. Der er en betydelig sammenhæng mellem god informationssikkerhed og efterlevelse af GDPR, og det kan derfor anbefales at se de to typer af tiltag under ét – f.eks. i form af ét regelsæt. Den dataansvarlige skal - især i store organisationer - være opmærksom på at sikre, at der er en passende funktionsadskillelse mellem dem, som bestemmer reglerne, og dem, som kontrollerer at reglerne efterleves og virksomheden er i compliance.

5. **Dokumentation af tilstand og tiltag**
   Der skal laves en fortegnelse over behandlingsaktiviteter, og det skal dokumenteres at alle behandlinger efterlever de grundlæggende principper. Det er derfor en god ide at lave en fortegnelse over informationsaktiver, som beskriver hvilke systemer man er i besiddelse af – inkl. dem der ligger hos outsourcingprovidere og i clouden – og tilknytte ejere til disse systemer. For hvert system kan man efterfølgende lave en kortlægning over behandlingsaktiviteterne. Man kan også lave kortlægningen af behandlingsaktiviteter på baggrund af de processer, som systemerne er en del af. Det anbefales at håndtere denne kortlægning i et dertil indrettet it-system, således at man er sikker på at komme hele vejen rundt i GDPR.

6. **Evaluering af lovligheden**
   På baggrund af kortlægningen eller i forbindelse med kortlægningen er det væsentligt at der foretages en vurdering af om behandlingsaktiviteterne er lovlige – har organisationen f.eks. fastsat et formål med en given behandling, forefindes et lovligt retligt grundlag for behandlingen, er den registrerede oplyst om behandlingen, slettes oplysningerne når behandlingens formål er opfyldt?

7. **Passende tekniske og organisatoriske foranstaltninger**
   På baggrund af risikovurderingen og kortlægningen af lovlige behandlinger i ovennævnte

fortegnelser kan man så iværksætte de foranstaltninger, som er nødvendige for at sikkerheden er optimal henset til de risici de registrerede står overfor. Tekniske foranstaltninger er f.eks. antivirus, firewall og automatisk opdatering. Organisatoriske foranstaltninger er f.eks. it-sikkerhedspolitikker og procedurer (regelsæt) samt oplysninger til kunder og medarbejdere om behandling af personoplysninger.

8. **Awareness**
   Uanset hvor mange foranstaltninger man iværksætter kan man ikke sikre sig fuldstændig mod den daglige behandling af personoplysninger. Det er derfor vigtigt, at der løbende sker en uddannelse af medarbejderne i forhold til, hvordan de håndterer personoplysninger. Der bør iværksættes løbende awareness-kampagner og testes i samarbejde med medarbejderne. Begge dele bør skræddersyes til hvad det er for oplysninger og behandlinger, som faktisk foregår i den konkrete organisation.

9. **Arbejdet slutter aldrig**
   Et GDPR-projekt afsluttes aldrig. Der vil ske en løbende justering af den juridiske praksis, der vil ske en løbende teknologisk udvikling og der vil ske en ændring i opfattelser af privatlivets fred. Det er derfor vigtigt at man løbende holder øje med udviklingen på området. Videre er det vigtigt, at det kontrolleres at regelsættene overholdes – det er ikke nok at skrive reglerne og implementere dem. Kontroller bør lægges ind i et årshjul, så der hver måned kontrolleres forskellige forhold – f.eks. hvor mange brugere har administratorrettigheder?, er udstyret faktisk opdateret med de seneste sikkerhedsopdateringer? og efterlever leverandørerne (databehandlerne) de aftaler, som der er indgået (databehandleraftalerne)?

Ovenstående kan synes som noget af en mundfuld. Organisationen skal være opmærksom på at skalere projektet, så det passer til organisationen og ikke bliver uoverkommeligt. Helt små organisationer, hvor alle kender hinanden, behøver således ikke lægge den store vægt på f.eks. punkt 1 og 2 ligesom mængden af systemer typisk vil begrænse sig til en håndfuld eller to.

Fastholde arbejdet med GDPR

Når en organisation er godt i gang med sit GDPR-projekt vil der typisk opstå en række udfordringer, som skal håndteres, for at sikre fremdriften og fremtiden.

1. **Langsigtet ansvarsplacering**
   Når arbejdet med GDPR går fra projekt til drift er det vigtigt fortsat at have en klar ansvarsplacering. Behandling af personoplysninger skal være forankret i organisationen, så der tages stilling til den løbende udvikling af arbejdsgange, procedurer, systemunderstøttelse, ibrugtagning af nye systemer, rapportering m.v. jf. nedenstående.

2. **Manglende bevillinger**
   I de fleste organisationer vil der være udfordring med at få de fornødne bevillinger til at gennemføre GDPR-projektet. Der er i de fleste organisationer sket en omfattende løbende digitalisering uden at der har været fokus på sikkerhed og beskyttelse af privatlivets fred. Der er således en god teknologigæld, der skal betales. Når der skal kommunikeres med ledelsen om bevillinger, er det vigtigt at bruges logiske argumenter (logos) som f.eks. henvisning til lovgivning, styring af sikkerhedsmæssige risici, god sikkerhed giver højere troværdighed hos kunder og

fremlæggelse af rapporter fra eksisterende sikkerhedsforanstaltninger. Det er imidlertid vigtigt også at bruges pathos, hvor man støtter sig op af udtalelser fra troværdige aktører som f.eks. Datatilsynet, Justitsministeriet, Center for Cybersikkerhed og RfDS og gengiver deres anbefalinger. Videre kan man med fordel også bruge en mere følelsesladet kommunikation (ethos), hvor man henviser til sikkerhedshændelser og bruger dem som cases i form af storytelling og også henviser til corporate sociale responsibility og de etiske aspekter af at beskytte personoplysninger og være en troværdig samarbejdspartner.

3. **Modvillige samarbejdspartnere**
   Der vil muligvis rundt omkring i organisationen være aktører, som synes at beskyttelse af personoplysninger er ligegyldigt og måske endda synes at det er bureaukratisk og mod organisationens interesser. Det er vigtigt at der gøres en ekstra indsats for at forklare nødvendigheden af GDPR-projektet overfor sådanne parter. Også her kan med fordel bruges logos, ethos og pathos. Det kan være nyttigt at have taget stilling til, i hvilket omfang modviljen skal have personale retlige konsekvenser. Modvillige samarbejdspartnere kan også findes i omverdenen. Overfor sådanne er det centralt at have en god forståelse af juraen og bruge den som argument.

4. **Problemer med implementering af foranstaltninger**
   Der vil typisk vise sig at være udfordringer med at implementere de fornødne foranstaltninger. Det kan f.eks. være at man har et ERP-system, hvor det ikke er muligt at implementere automatisk sletning, når formålet er opfyldt. Det kan også være at der er udfordringer med at få en konkret overvågningsteknologi til at virke i ens infrastruktur. Det er vigtigt at sådanne udfordringer kortlægges, og at der træffes beslutninger, som sikrer, at projektet forsætter af det planlagte spor og ikke bare henlægges med manglende compliance med GDPR til følge.

5. **Ændring af praksis**
   Over tid vil praksis ændre sig, og ny praksis kommer til i takt med, at beslutningstagere bliver klogere. Det er vigtigt at følge med i disse ændringer og have en proces, som sikrer, at der samles op på disse ændringer og at kortlægning og procedurer i organisationen opdateres.

6. **Ændring a system-setup m.v.**
   Også systemlandskabet ændrer sig over tid. Nye systemer, ny teknologi, nye medarbejdere, nye leverandører er en del af dagligdagen. Det er vigtigt at dokumentationen løbende opdateres i takt med disse ændringer og ikke over tid sander til og bliver forældet. Der skal derfor være en proces i organisationen, som sikrer at det indrapporteres til GDPR-projektlederen, hvad der skal af ny udvikling overalt. Projektlederen skal også selv søge nye informationer. Det er nyttigt, hvis projektlederen har adgang til tekniske foranstaltninger, som kan medvirke til at afsløre denne type ændringer.

7. **Kontroller**
   ”Hvis det ikke er dokumenteret og kontrolleret, er det ikke gjort”. Det er ikke nok at have en papirtiger af dokumentation og regler liggende, hvis det ikke løbende kontrolleres, at reglerne efterleves. Det skal derfor udpeges en person, som sikrer, at det kontrolleres og dokumenteres at reglerne efterleves, og at der foretages kontrol af de aftaler, der er indgået med databehandlere. I fald reglerne ikke efterleves, skal der rapporteres til GDPR-projektlederen og ledelsen, som så må

iværksætte de rette korrigerende tiltag. Den dataansvarlige skal besluttede et rimeligt niveau for de kontroller, de ønsker at gennemføre.

Konklusion

RfDS er fuld bevidste om, at der er mange måder at drive sit GDPR-projekt på. RfDS har med denne vejledning forsøgt at skitsere nogle af de centrale elementer, som en organisation bør gennemløbe. Det er imidlertid centralt, at enhver organisation tilpasser den ovenstående skitse til sin egen organisation, for at opnå det bedst tænkelige GDPR-projekt.