Rådet for Digital Sikkerhed

april 2019

Rådets dataetiske principper

- tjekliste ved lovforslag og konkrete digitale initiativer mv.

Rådet for Digital Sikkerhed finder det vigtigt, at borgerne kan have tillid til, at deres oplysninger behandles lovligt, rimeligt og etisk. Rådet for Digital Sikkerhed anbefaler derfor, at beslutningstagere, som stiller forslag om ny lovgivning, nye digitale løsninger eller ønsker et givent formål opfyldt med digitale midler, gennemgår nedenstående liste og vurderer, om tiltaget kan opfyldes indenfor disse ti principper:

1. **NØDVENDIGHED**
   Er det umuligt at opfylde formålet med løsningen helt uden at indsamle personoplysninger eller med fuld anonymisering af data?
   (hvis nej, så vælg at re-designe løsningen)
2. **LOVLIGHED**
   Er der fuld klarhed over hjemmelsgrundlaget?
   (er metoden lovlig pga. samtykke, legitime interesser, kontrakt eller særlov)
3. **ETISK DESIGN**
   Sikres individets rettigheder og principperne i GDPR gennem it-løsningens design?
   (forudbestemt formål, kun indsamling af nødvendige data, indsigt, oplysningspligt, kontrol over egne data, sletning m.v.)
4. **KONSEKVENSER**
   Er der på forhånd taget stilling til, hvilke konsekvenser forslaget/løsningen kan have for de registrerede på kort og på lang sigt?
5. **VALGFRIHED**
   Er det valgfrit for den enkelte, hvorvidt data om vedkommende registreres eller ej?
6. **SIKKERHED**
   Er der etableret en passende sikkerhed i og omkring systemet i tråd med de nødvendige og bedst tilgængelige tekniske og organisatoriske metoder?
7. **TRANSPARENS**
   Er der gennemsigtighed i behandlingen, herunder ved brug af algoritmer og er der menneskelig kontrol med resultaternes rimelighed?
8. **RESPEKT FOR MENNESKERETTIGHEDER**
   Er der sikkerhed for, at databehandlingen ikke er bias med risiko for diskriminering, marginalisering eller stigmatisering af individer?
9. **PROPORTIONALITET**
   Er der foretaget en proportionalitetsafvejning og dermed sikret, at individets rettigheder ikke undermineres ud fra en "målet helliger midlet" tankegang?
10. **ANSVARLIGHED**
    Er der klarhed om ansvarsplacering, løbende tilsyn og klageadgang?

Rådet for Digital Sikkerhed

april 2019

Baggrund

Personoplysninger er en vigtig kilde til at udvikle digitale tjenester og opfylde kommercielle, politiske og samfundsrelevante formål. Det er derfor relevant for både virksomheder, myndigheder og organisationer at indsamle og behandle personoplysninger.

Det kan være helt legitimt at ønske at behandle personoplysninger, men det ændrer ikke ved, at behandlingen skal vurderes i forhold til en række lovgivningsmæssige og etiske principper.

Som det følger af Grundlovens § 72, Verdenserklæringen om menneskerettigheder artikel 12, Den Europæiske Menneskerettighedskonvention artikel 8 og Den Europæiske Unions Charter om Grundlæggende Rettigheder artikel 8 har individet ret til privatlivsbeskyttelse.

Denne ret er dog ikke ufravigelig, men det er Rådet for Digital Sikkerheds (RfDS) opfattelse, at skal man fravige retten, er det vigtigt, at det sker på baggrund af en grundig analyse, hvor man har vurderet, om man kan opnå sit formål på en mindre indgribende måde.

RfDS må konstatere, at der med mellemrum fremsættes forslag, hvis formål måske nok er ædle, men hvor der ikke er foretaget en vurdering af, om man kunne opnå det samme formål med mindre indgribende midler.

Som eksempler kan nævnes forslag til ændring af Loven om Center for Cyber Sikkerhed, den såkaldte 'Gladsaxemodel', trivselsundersøgelser i skolevæsnet og sagen om udvidelsen af diagnoser registreret i Den Almen Medicinske Database (DAMD).

Der findes en lang række teknologiske muligheder, som i høj grad overses i en politisk kontekst, når der laves forslag som indebærer behandling af personoplysninger. Disse omfatter blandt andet anonymisering, pseudonymisering og multiparty computation (brug af flere identiteter).

Det er denne type af teknologier, som RfDS ønsker i højere grad bringes i anvendelse til at understøtte retten til privatlivsbeskyttelse.

Dataetiske principper til vurdering af nye datainitiativer

RfDS har derfor præciseret hvilke principper, der bør skeles til, når der fremsættes nye forslag eller tages initiativ til at bruge nye digitale løsninger. En række af disse forslag følger allerede af den eksisterende persondataret. Det er centralt, at politiske beslutningstagere ikke tilsidesætter disse principper med deres forslag.

For at undgå at blive mødt med forslag, som unødvendigt tilsidesætter individets ret til privatlivsbeskyttelse, har RfDS lavet denne tjekliste som beslutningstagere, når de overvejer, om de opnår et givent formål uden at tilsidesætte individets privatlivsbeskyttelse kan benytte sig af – og dermed balancere hensigten/målet optimalt i forhold til de anvendte midler.

Rådet for Digital Sikkerhed anbefaler derfor, at alle 10 spørgsmål kan besvares med et JA, førend et lovforslag eller en konkret it-løsning iværksættes.