DATAETHICS

DataEthics.EU arbejder for at fremme dataetiske produkter og tjenester med en vision om at flytte den digitale forretningsmodel fra tracking-by-default til privacy-by-default. Vi deler viden omkring dataetik og dataanvendelse for virksomheder, uddannelsesinstitutioner, organisationer, individer og beslutningstagere.

EU's forordning om persondatabeskyttelse

Af Birgitte Kofod Olsen, der har en juridisk PhD-grad i persondatabeskyttelse, er medstifter af DataEthics.EU og til daglig partner i konsulentvirksomheden Carve.

EU's forordning om persondatabeskyttelse har et markant fokus på databeskyttelse som grundrettighed. EU Charteret for grundrettigheder indeholder nemlig retten til **persondatabeskyttelse som en selvstændig rettighed** ved siden af retten til respekt for privatlivet. Med forordningen får disse grundrettigheder et konkret indhold, der forpligter alle aktører i den offentlige og private sektor til at værne om persondata. Samtidig er det lykkedes at skrue en forordning sammen, der taler ind i virksomheders dagligdag; der er fokus på sikkerhed, risikoafdækning og -styring, på leverandørforhold og på dokumentation. Det gør det muligt at **integrere databeskyttelse i eksisterende processer** og rutiner, hvilket i sig selv bidrager til bedre beskyttelse af persondata.

Indhold

Fokus på individet

Behandling af personoplysninger bør have til formål at tjene menneskeheden

Beskyttelsen af individet står centralt og præger både forordningens krav til databehandling og det niveau, der er valgt for **administrative bøder som sanktion** for manglende opfyldelse af forordningen. Det er højt, helt op til 20 mio euro eller for virksomheder 4% af den årlige omsætning. Det signalerer alvorlighed. I præamblen til forordningen slås det da også fast, at "Behandling af personoplysninger bør have til formål at tjene menneskeheden". Det har som konsekvens at kravene til persondatabeskyttelse bliver strengere og at der bliver stillet større krav til virksomhedernes dataansvarlighed. De hovedprincipper om fairness og transparens, som forordningen hviler på, lægger således en dataetisk dimension til al persondatabehandling, ligesom det mere håndfaste krav om dokumentation af databehandlingen i praksis vil betyde, at virksomheder og myndigheder skal have overblik over deres it-arkitektur og de data flows, som persondata indgår i, både internt og med eksterne samarbejdspartnere. Det samme gør de **skrappere krav til databehandlere.**

Dataansvarlighed

..det eksplicitte krav, at den dataansvarlige skal implementere en persondatapolitik

De bærende principper for al persondatabehandling er, at behandlingen er lovlig og rimelig, og også fremstår for datasubjektet på en gennemsigtig måde. Borgere og kunder skal med andre ord kun acceptere en behandling af deres data, som passer til deres rimelige forventninger, og som foregår på en måde, der giver indblik i, hvordan og til hvilket formål data behandles. At behandlingen skal være lovlig er åbenbar, men der gemmer sig en række specifikke krav til det lovlige grundlag for databehandlingen, som nævnes nedenfor.

Principperne om lovlighed, rimelighed og gennemsigtighed udgør kernen i det krav til *dataansvarlighed* (accountability), som EU forordningen knæsætter som en ny standard for databehandling. Forankret i dataansvarligheden opstiller EU forordningen således en række krav til virksomheder og myndigheders organisatoriske foranstaltninger. Nogle er knyttet til intern regulering, mens andre berører roller og funktioner i forhold til databehandlingen.

Blandt de første er det eksplicitte krav til den dataansvarlige **om at implementere en persondatapolitik** (artikel 24). Det skal læses i sammenhæng med de krav, der pålægges den dataansvarlige i forhold til at sikre sin egen og databehandleres overholdelse af forordningen (artikel 28) samt kravet om at føre fortegnelser over databehandlingen (artikel 30), også kaldet dokumentationskravet.

Opfyldelse af disse krav forudsætter, at **virksomheden eller myndigheden har beskrevet og vedtaget processer** og procedurer, der dels fastlægger roller og ansvar for medarbejdere og funktioner, der udfører databehandling, dels identificerer de godkendte adfærdskodekser og certificeringer (artikel 24) eller andre tekniske standarder, som virksomheden anvender til styring og kontrol af deres databehandling.

Databeskyttelsesrådgiver

En ramme, der sikrer de rette kompetencer og skaber en databeskyttelseskultur

Introduktionen af en **ny funktion som databeskyttelsesrådgiver** afspejler også det overordnede princip om dataansvarlighed. Myndigheder og de virksomheder, som er involveret i regelmæssig og systematisk overvågning af datasubjekter i stort omfang eller behandling af følsomme persondata og oplysninger vedrørende strafbare forhold skal udpege en databeskyttelsesrådgiver. Den person, der udpeges, har til **opgave at underrette og rådgive den dataansvarlige** eller databehandleren og de ansatte om deres forpligtelser efter forordningen og anden lovgivning, og også overvåge at lovgivning og interne politikker om databeskyttelse overholdes (artikel 37).

Til opgaven som databeskyttelsesrådgiver knytter sig også opgaver som **oplysningskampagner og uddannelse af medarbejdere**, der behandler persondata. Ved at medtage sådanne opgaver i forordningen skabes der en ramme, der ikke blot pålægger retlige forpligtelser til at sikre databeskyttelse, men sikre de rette kompetencer hos medarbejderne og skaber en databeskyttelseskultur.

Konsekvensanalyser

Forordningens ambitionsniveau kommer særligt tydeligt til udtryk i kravet til den dataansvarlige om at **udarbejde analyser af, hvilke konsekvenser databehandlingen har** for borgernes og kundernes rettigheder og frihedsrettigheder i bred forstand (artikel 35).

Med kravet indføres et risikoparadigme i forhold til databeskyttelse, som mange virksomheder vil være fortrolig med, fordi det allerede anvendes i forhold til forretningsrisici og sikkerhedsrisici. Eksisterende redskaber til afdækning af aktuelle og potentielle risici, vurdering af sandsynligheden for, at de opstår, samt planer for migrering, eliminering, forebyggelse samt kontroller og beredskab vil derfor kunne anvendes.

Det nye element er, at der nu også skal være **fokus på den risiko, der er for at påvirke borgerne**/kundernes rettigheder negativt. Og det er en temmelig omfattende opgave, når det rettighedskatalog, der ligger bag formuleringen ”rettigheder og frihedsrettigheder”, består af EU Charter om grundrettigheders 54 bestemmelser.

Design og standardindstillinger

Krav om, at indlejre persondatabeskyttelse i designet af it-løsninger

Et stort skridt i retning af effektiv beskyttelse af persondata tages med forordningens krav om, at myndigheder og virksomheder skal sørge for at **indlejre persondatabeskyttelse i designet** af it-løsninger til persondatabehandling (artikel 25). Det betyder, at man fx skal vurdere, om det er nødvendigt at anvende pseudonymisering og dataminimering for at beskytte datasubjektet grundrettigheder. Den vurdering skal foretages både på tidspunktet for valg af it-løsninger til databehandlingen og på tidspunktet for selve behandlingen. I tilknytning til designet af databehandlingen skal man også tage stilling til, om anvendelse af standardindstillinger i it-løsningen kan sikre, at der **kun anvendes persondata, der er nødvendige til hvert specifikt formål** med behandlingen.

Implementeringen af disse krav forudsætter, at organisationen er parat til at løfte opgaven, både organisatorisk, d.v.s. i forhold til beslutningsprocesser og kompetencer, men også i forhold til etablering og udvikling af passende tekniske løsninger og udstyr.

Betingelser for databehandlingen

Persondata må ikke viderebehandles på en måde, der er uforenelig med det oprindelige formål

EU forordningen fastslår som det tidligere gældende direktiv en række betingelser, der skal være opfyldt, når der behandles persondata (artikel 5). **Persondata må kun indsamles til bestemte og lovlige formål** (*formålsbestemthed*), og **må ikke viderebehandles på en måde, der er uforenelig med det oprindelige formål** *(formålsbegrænsning).* Formålsforskydning er dermed ikke udelukket, men det kræver en konkret vurdering af, om der er forenelighed mellem det nye og det oprindelige formål med dataindsamlingen.

De persondata, der anvendes til at opfylde formålet, **skal være relevante, tilstrækkelig og nødvendige** *(dataminimering)*, de skal være korrekte og opdaterede, og myndigheden eller virksomheden skal selv tage rimelige skridt til berigtige elle slette data, der er ukorrekte. *(rigtighed)*. Persondata må kun opbevares i den periode, hvor de er nødvendige i forhold til at opfylde formålet, og skal herefter slettes *(opbevaringsbegrænsning),* og de skal under alle dele af behandlingen sikres mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse *(integritet og fortrolighed).*

Det er til enhver tid den dataansvarlige, der er ansvarlig for, at disse behandlingsbetingelser er opfyldt, også hvor hele eller dele af databehandlingen er outsourcet til en leverandør eller samarbejdspartner.

Samtykke og andre lovlige grundlag

I praksis skal den dataansvarlige udforme en samtykkeerklæring i en letforståelig og lettilgængelig form og i et klart og enkelt sprog.

Behandling af persondata skal fortsat have et lovligt grundlag. På grund af forordningens fokus på den individuelle ret til databeskyttelse, er datasubjektets samtykke udgangspunktet for enhver databehandling.

Andre lovlige grundlag kan imidlertid tilsidesætte samtykkekravet. Det kan fx være en kontrakt, som datasubjektet er part i, eller at lovgivningen indeholder et krav om behandling af persondata, som den dataansvarlig skal opfylde. Hvis databehandlingen sker for at beskytte datasubjektets eller en anden fysisk persons vitale interesser eller for at udføre en opgave i samfundets interesse kan dette også udgøre det lovlige grundlag. Endelige kan databehandlingen være knyttet til **en legitim interesse hos den dataansvarlige eller en tredjemand, som må anses at veje tungere** end hensynet til datasubjektets interesser og rettigheder (artikel 6)

Ved behandling af særlige kategorier af persondata, d.v.s. oplysninger, som vurderes som følsomme på grund af deres indhold, fx om etnicitet, politisk ståsted, religion, sundhed og seksuel orientering, skal vurderingen tage afsæt i, at behandling som udgangspunkt er forbudt. Behandling kan derfor kun iværksættes undtagelsesvis og kræver i så fald et udtrykkeligt samtykke fra datasubjektet. Det kan være bestemt ved lov, at samtykkekravet ikke kan hæves, men der kan også være skabt hjemmel til, at samtykkekravet kan erstattes af andre lovlige grundlag, herunder datasubjektets vitale interesser, en væsentlig samfundsinteresse, fx i folkesundhed, eller for at den dataansvarlige kan opfylde sine arbejds-, sundheds- og socialretlige forpligtelser eller for at gøre retskrav gældende ved domstolene. Hvis datasubjektet selv har offentliggjort følsomme data om sig selv, må de også behandles uden samtykke, hvis det er tydeligt, at det er datasubjektet selv, der står bag offentliggørelsen (artikel 9).

Den dataansvarlige skal kunne påvise, at datasubjektet har givet sit samtykke til databehandlingen (artikel 7). **Samtykkekravet bliver dermed et krav om *aktivt* samtykke**. Det vil derfor ikke være nok, at der oplyses om anvendelsen af persondata og at manglende indsigelse eller anden aktivitet fra datasubjektet mod databehandlingen, ses som udtryk for, at vedkommende samtykker. I praksis vil den dataansvarlige typisk skulle udforme en samtykkeerklæring og stille den til rådighed i en letforståelig og lettilgængelig form og i et klart og enkelt sprog. Samtykket skal også være afgivet frit og på et informeret grundlag. For at sikre, at samtykket er informeret, bør datasubjektet som minimum være bekendt med den dataansvarliges identitet og formålene med den behandling, som vedkommendes persondata anvendes til. Hvis datasubjektet ikke har et reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende, kan et samtykke ikke anses som afgivet frivilligt.

Datasubjektets rettigheder

Datasubjektet har ret til at få berigtiget urigtige oplysninger og få slettet data, der fx er unødvendige i forhold til formålet eller er ulovligt behandlet

Forordningen indeholder et katalog af rettigheder for datasubjektet, som bidrager til at give vedkommende indsigt i databehandlingen og adgang til egne data. Datarettighederne er med til at understrege forordningens fokus på individets databeskyttelsesret.

Kataloget indeholder retten til at få oplysninger om den dataansvarliges identitet, hvor dataene er indhentet, hvilket formål, de anvendes til, hvad det lovlige grundlag for behandlingen er, hvor længe data opbevares og om de overføres til et tredjeland.

Hvis data anvendes til træffe automatiske afgørelser, fx på baggrund af profilering datasubjektet, skal dette også oplyses. Derudover skal der oplyses om muligheden for at klage over databehandlingen. (art. 13 og 14) Som en refleksion af denne oplysningspligt for den dataansvarlige, har datasubjektet også en indsigtsret, der giver vedkommende ret til at få bekræftet om en dataansvarlig behandler data om dem og hvordan behandlingen foregår samt at modtage oplysninger om klageadgang (artikel 15).

Datasubjektet har derudover **ret til at få berigtiget urigtige oplysninger** (artikel 16) og - som den mest omtalte rettighed – **retten til at blive glemt**, d.v.s. til at få slettet data, der fx er unødvendige i forhold til formålet eller er ulovligt behandlet, uden unødig forsinkelse (artikel 17). Man har også ret til at få begrænset databehandlingen, fx hvis dele af den er ulovlig eller datasubjektet bestrider rigtigheden af de anvendte data (artikel 18).

Forordningen indeholder også et par nyskabelser. Den ene er **retten til dataportabilitet**, som giver datasubjektet **ret til at modtage** de **data**, han eller hun har givet til den dataansvarlige, **og til at få dem transmitteret til en anden dataansvarlig**. Data skal stilles til rådighed i et struktureret, almindeligt anvendt og maskinlæsbart format og overføres direkte til den dataansvarlige, som datasubjektet udpeger (artikel 20).

Den anden nyskabelse er **retten til at gøre indsigelse mod profilering**. Det kan ske, når persondata behandles med henblik på direkte markedsføring. Datasubjektet har i sådanne situationer ret til at gøre indsigelse mod behandlingen på ethvert tidspunkt og databehandlingen skal i så fald ophøre (artikel 21).

Samlet set vil realiseringen af datarettighederne give store udfordringer i praksis. En ting er at skabe en it-arkitektur og datasæt, der gør det muligt at udtrække alle data på personniveau og give adgang til dem, en anden ting er overføre et sæt kundedata til en anden dataansvarlig, som vil kunne være en konkurrent. Det må forventes at disse tekniske og forretningsmæssige barrierer i en vis grad vil hæmme en effektiv beskyttelse af datasubjektet.

Sikkerhed

Det er også nyt, at den dataansvarlige skal anmelde brud på persondatasikkerheden til Datatilsynet

EU forordningen hæver også beskyttelsesniveauet gennem kravene til sikkerhed. Sikkerhedsniveauet og behandlingssystemernes robusthed skal således vurderes i forhold til de risici, som behandlingen af persondata giver anledning til, i forhold til at påvirke datasubjektets rettigheder og frihedsrettigheder negativt.

Vurderingen er kontekstbestemt og kan derfor inddrage både virksomhedens eller myndighedens tekniske niveau, de implementeringsomkostninger, der vil være forbundet med at øge sikkerheden, fx gennem pseudonymisering og kryptering, men også selve databehandlingens karakter og omfang.

Sikkerhedsforanstaltningerne skal sikre fortrolighed, integritet, tilgængelighed og behandlingssystemer og -tjenesters robusthed, og skabe sikkerhed for rettidig genoprettelse af tilgængelighed og adgang til persondata efter en fysisk eller teknisk hændelse.

De organisatoriske krav til at opbygge sikkerhed omfatter procedurer for regelmæssig afprøvning, vurdering og evaluering af sikkerhedsforanstaltningernes effektivitet. Der skal også føres kontrol med, at de fysiske personer, der udfører arbejde for den dataansvarlige og for databehandleren, kun får adgang til persondata efter instruks fra den dataansvarlige (artikel 32).

Det er også nyt, at **den dataansvarlige skal anmelde brud på persondatasikkerheden til Datatilsynet**. Det skal ske uden unødig forsinkelse og **senest 72 timer efter** bruddet. Anmeldelse kan dog undlades, hvis bruddet ikke indebærer risiko for fysiske personers rettigheder og frihedsrettigheder.

En forudsætning for at kunne vurdere dette **er**, at man har sin **konsekvensanalysen** er på plads. I tilknytning hertil skal den dataansvarlige dokumentere alle brud på persondatasikkerheden, herunder de faktiske omstændigheder, bruddets virkninger og de trufne afhjælpende foranstaltninger (artikel 33).

Den dataansvarlig skal også uden unødig forsinkelse underette datasubjektet om bruddet på persondatasikkerheden, hvis det indebærer en høj risiko for deres rettigheder og frihedsrettigheder (artikel 34).

En nødvendig helhedsorientering

Det drejer sig ikke kun om overholdelse af lovgivning, men også om forretningsmæssige risici

Med forordningens krav til betingelserne for databehandling og dens lovlige grundlag, samt til de anvendte tekniske midler, herunder kryptering og pseudonymisering, men også til indlejring af persondatabeskyttelse i designet af behandlingssystemer, bidrager den til at omsætte grundrettighederne til privatlivsbeskyttelse og persondatabeskyttelse til praksis i myndigheder og virksomheder.

Det er også et stort skridt fremad, at der nu stilles krav til den organisatoriske ramme, herunder til vedtagelse af persondatapolitik og brug af godkendte adfærdskodeks og certificeringer samt til procedurer for sikkerhedshåndtering.

De nye krav til persondatabeskyttelse nemlig på den måde relevante i dagligdagen for alle områder i en virksomhed, både udvikling, BI, salg og marketing, drift af hjemmesider, kundeservice og administration. Tilsvarende gælder for offentlige myndigheder.

Samlet set indfører forordningen en helhedsorientering på persondatabeskyttelsesområdet. **Det drejer sig** ikke længere kun om overholdelse af lovgivning, men **også om forretningsmæssige risici**, om valg af **de rigtige it-løsninger og leverandører**, om formaliserede processer og procedurer, og om **kompetence- og en sikkerheds og persondatakulturudvikling**.