

Nytt personvernregelverk:

# Dataportabilitet

Personvernforordningen (EU 2016/679, GDPR) lanserer et helt nytt begrep i personvernsammenheng, nemlig retten til dataportabilitet. Hva betyr det for virksomheter å måtte gi fra seg personopplysninger i maskinlesbart format?



Advokatfullmektig  
**Charlotte Elise Thuesen**  
Deloitte Legal



Advokat  
**Bjørn Ofstad**  
Deloitte Legal

Har en virksomhet registrert og lagret informasjon om deg, har du i dag en rett til å få vite hvilken informasjon virksomheten (behandlingsansvarlig) har lagret om deg – og hva de bruker denne informasjonen til. Videre har du etter forespørsel en rett til å få disse opplysningene utlevert. Dette er rettigheter basert på gamle personvernprinsipper og som videreføres i nytt personvernregelverk. Opplysninger om en selv tilhører den enkelte og best kontroll over egne opplysninger gir best personvern.

Dagens personvernregelverk stiller ingen krav til formen slik informasjon skal leveres i – og vi har vel alle hørt historier om de som har bedt om informasjon og fått utdelt ti kilo med papir. Ny personvernlovgivning som trer i kraft mai 2018 vil gi den registrerte, det enkelte individet, sterkere rettighet enn før i denne sammenheng. En av de nye rettighetene er dataportabilitet, noe som vil gjøre det mulig for den registrerte å kreve data utlevert i et format som er strukturert, alminnelig anvendt og maskinlesbart. Dette vil også bety at man faktisk kan bruke disse dataene til noe, i motsetning til slik det er i dag hvor man risikerer å bli sittende med en stor papirbunke.

Retten til Dataportabilitet medfører også at individer kan ta med seg sine data mel-

lom forskjellige systemer og tjenester, en rettighet vi tror i stadig større grad vil bli applaudert av samfunnet.

## En ny rettighet

Retten til dataportabilitet vil gi eieren av dataene større mulighet til å bruke sine egne data til det man selv ønsker. Individet kan eksempelvis velge å beholde dem selv, gi dem videre til en konkurrerende tjenesteleverandør, eller til og med kreve dem direkte overført fra en virksomhet til en konkurrent – såfremt det er teknisk mulig.

Retten til dataportabilitet er begrenset til et snevrere omfang av opplysninger sammenlignet med den eldre retten til informasjon fra virksomheten. Dataportabilitet gjelder kun for opplysninger som behandles elektronisk og kun opplysninger som er samlet inn med grunnlag i samtykke eller

kontrakt. I tillegg gjelder det kun opplysninger individet selv har gitt fra seg; «provided by the individual», som det heter i forordningsteksten. Opplysninger som individet selv aktivt har gitt fra seg, for eksempel via et skjema, er typisk omfattet.

Retten til dataportabilitet kan også være nyttig for den registrerte når det gjelder opplysninger som gir en tilbudt tjeneste en ekstra verdi for brukeren. Eksempelvis vil opplysninger som individet gir fra seg indirekte, også være omfattet av retten til dataportabilitet. Dette betyr at data som søkehistorie, lokasjonsdata og informasjon i en tracker, som genereres ved bruk av tjenesten, eksempelvis data som søvnvaner, hjerteslag eller treningsøkter, som genereres gjennom bruk av en tjeneste, kan kreves flyttet. Transaksjonsdetaljer og mobilforbruk, og til og med e-poster kan også tenkes overført under denne rettigheten.



Retten til dataportabilitet vil gi eierne av data større mulighet til å bruke sine egne data til det de selv ønsker.

Grensene for data som kan kreves tatt med videre, er i skrivende stund ikke endelige. Vi vet det går en grense for data som ikke kan kreves utlevert når tjenesteleverandør har tolket dataene, eller når tjenesteleverandøren har behandlet dataene på en eller annen måte. Personalisering, redaksjonelt og skreddersydd innhold, personlige anbefalinger og profiler, er eksempler på andre typer data som ikke er å anse som inngitt av individet og som derfor heller ikke er underlagt retten til dataportabilitet. Dette viser oss at det kan være krevende å avgjøre hvilke data som omfattes av prinsippet om dataportabilitet og hvor konkrete vurderinger er nødvendige.

### Konkurransfordel – utfordringer

Hovedformålet med personvernregelverket, og i dette tilfellet dataportabilitet, er å gi individer bedre kontroll og råderett over egne personopplysninger. For virksomhetene medfører dette, slik vi ser det, både tekniske og organisatoriske utfordringer. På den annen side kan retten til dataportabilitet også være en konkurransefordel, noe vi tror vil bli verdsatt av mindre virksomheter i en oppstartsfase i kampen mot de etablerte virksomhetene. Retten til dataportabilitet vil gjøre det enklere for den enkelte å gå over til en konkurrerende virksomhet med mer passende produkter, eller rett og slett fordi de tilbyr bedre personvern.

Fremover blir lock-in i systemer både svært upraktisk og lite fristende for forbrukere. Forbrukere ønsker å bruke sine egne data til å sammenligne tjenester mot hverandre, kanskje oppnå rabatter på grunn av et bestemt bruksmønster, og få tilpassede tjenester fra dag én hos en ny aktør. En virksomhet kan, slik vi ser det, ved hjelp av tiltransporterte data tilby persontilpasset bilforsikring basert på kjøremønsteret, eller kanskje basere kredittvurderingen på atferdsdata fra sosiale medier. Datatilsynet uttaler i sin årlige utgivelse om tilstand og trender for personvern i 2017 at «ditt liv på nett kan bestemme prisen på tjenesten». Mulighetene som dataportabilitet gir er spennende og vil garantert gi flere muligheter (og utfordringer) enn vi klarer å se for oss pr. i dag.

### Etterlevelse

Det er ikke lagt inn noen særskilte unntak for virksomhetens plikt til å etterleve dataportabilitet, og minimumskravet om mas-

kinlesbart format skal være relativt enkelt å imøtekomme.

Dataportabilitet må likevel fungere teknisk slik at virksomheten er i stand til å flytte på dataene. Etablerte aktører må, sett hele det nye regelverket under ett, tenke «privacy by design» på allerede etablerte strukturer. Nye aktører kan tenke dette fra dag én.

Et sentralt spørsmål er i hvilken grad virksomheten må bygge opp kompatible systemer og forplikte seg til at systemene passer med andre. Dette er først og fremst noe virksomhetene i dag oppfordres til, ikke pålegges, og det er konkrete vurderinger som hver virksomhet må gjøre seg over hvor langt de skal tilpasse egen virksomhet. Flere bransjer er utsatt for disruptive teknologiske strømmer fra flere hold.

Revisjonen av betalingstjenestedirektivet, som også er aktuelt i Norge fra 2018, medfører at tredjeparter snart kan bygge egne tjenester på toppen av bankenes data og infrastruktur. Disse tredjepartsleverandørene vil kunne måtte få tilgang til kundenes kontoer og tilsvarende være aktuelt for kravet om dataportabilitet.

Teknologien er derfor enten allerede på plass, eller ikke langt unna, for at også kravet om dataportabilitet kan oppfylles innen flere sektorer. Noe som også er hensikten.

### Forberedelser

Virksomheter må begynne å tenke personvern i alle ledd, personvern og «Privacy by design», eller innbygget personvern, har kommet for å bli.

Innebygget personvern handler i korte trekk om å ta hensyn til personvern i alle faser, prosesser og systemer. Hittil har dette kun vært anbefalt som beste praksis, men blir i nytt personvernregelverk påbudt. Det er virksomheten sitt ansvar at kun de korrekte dataene deles ut. Det betyr at man må kunne segmentere ut hvert individ sine data. Denne forutsetningen ser vi er gjennomgående for flere av kravene i forordningen, og ved neste oppdatering av IT-systemet bør en sørge for at personopplysninger kan segmenteres, slettes, og hentes ut.

Virksomhetene må også være i stand til å håndtere henvendelser fra kundene om dette. For dataportabilitet kan man vurdere å gjøre dette så enkelt at individer kan ta ut de dataene de vil selv, ved å ha en «last ned»-knapp tilgjengelig. Dette gjøres i flere tjenester på eget initiativ allerede, nettopp fordi det gir god kundetilfredshet. Se for dere at kunden kommer og sier at de vil ta med transaksjonsdetaljer ved bytte av bank, dataforbruk på mobilen for å få bedre tilbud på datapakke fra ny teleoperatør, eller de selvlagde spillelistene fra en musikkjeneste til en annen. Klarer din virksomhet å ta imot slike henvendelser?

På den andre siden må virksomheten kunne ta imot data som kundene tar med seg fra andre tjenester. Ved tiltransporterte data kan det også være behov for en enkel måte å innhente samtykke på, for eksempel ved å bruke et samtykkeverktøy for innhenting og dokumentasjon, slik at de mottatte personopplysningene kan brukes til noe.

Vi mener godt personvern er et konkurransefortrinn. Nytt personvernregelverk kommer, og det kommer allerede mai 2018.

## AKTUARBEGNINGER OG TJENESTER

Kollektiv pensjonsforsikring.  
Aktuarberegning av pensjonsforpliktelser utføres av NIA til konkurransedyktige priser. Hurtig leveringstid.

### NIA – Nordic Insurance Administration AS

Forskningsparken –Gaustadalleen 21 – 0349 Oslo  
Tlf: 99 56 89 48 – E-post: nia@aktuar.com