DATATILSYNETS STRATEGI

1. januar 2018 - 31. desember 2020

Datatilsynet

Innhold

Om strategien **4**

Datatilsynet – roller og virkemidler **5**

Våre verdier **7**

Hva er personvern? **8**

Omverdensanalyse – personvern er viktigere enn noensinne **12**

Strategiske mål **18**

Om strategien

Denne strategien trer i kraft like før et nytt personvernregelverk implementeres i Europa i mai 2018. Samtidig opplever vi at bruken av personopplysninger intensiveres både i offentlig og privat sektor. Datatilsynet merker stor pågang av spørsmål, saker og mediehenvendelser om det nye regelverket, og om håndtering av personopplysninger generelt.

I en situasjon der personvernhensyn blir enda viktigere og der vi opplever stort arbeidspress, må vi prioritere ressursene våre på en god måte. Målet med denne strategien er å peke ut en klar retning for arbeidet vårt og å være ambisiøse for å sikre godt personvern.

Vi har hentet inspirasjon internt og eksternt i utviklingen av strategien. Vi har gjennomført en SWOT-analyse der alle medarbeiderne i Datatilsynet har identifisert styrker, svakheter, muligheter og utfordringer for personvernet generelt og for tilsynet spesielt. Denne analysen har vært utgangspunktet for arbeidet med strategien.

Som en del av strategiprosessen har vi hentet innspill fra en rekke eksterne aktører, og vi har hatt rundebordsmøter med virksomheter fra både offentlig og privat sektor. Dette var en viktig del av vår vurdering av risikoer og muligheter for personvernet i norsk kontekst. På bakgrunn av dette har vi utarbeidet en omverdensanalyse som har vært avgjørende i valg av strategiske mål.

Internt i Datatilsynet har vi hatt flere samlinger der vi har diskutert tilsynets verdigrunnlag og hvordan vi best kan bruke vår rolle som tilsyn og ombud til å fremme godt personvern. Vi har sett fremover mot det nye regelverket og hvordan dette vil påvirke vår måte å jobbe på.

Personvernlandskapet er i stadig endring, og det er viktig at Datatilsynet jobber langsiktig og strategisk, holder seg oppdatert på teknologitrender og sørger for å være godt synlig. I denne strategien har vi utviklet seks mål som viser hvilken retning vi skal gå de neste tre årene. Målene skal operasjonaliseres i tilsynets virksomhetsplan i hvert av de tre årene strategien gjelder.

Datatilsynet – roller og virkemidler

Datatilsynets viktigste oppgave er å føre tilsyn med blant annet personopplysningsloven, helseregisterloven og pasientjournalloven. Vi er et særskilt uavhengig forvaltningsorgan under Kommunal- og moderniseringsdepartementet, og kan ikke instrueres av departementet i enkeltsaker. Vi beslutter selv hvilke sektorer vi prioriterer og hvilke arbeidsmetoder vi velger å bruke.

En annen viktig oppgave for oss, er å være ombud i personvernspørsmål. Vi skal delta i personverndebatten, undersøke og dele fakta om personvernets kår både nasjonalt og internasjonalt, og jobbe for at personvernet ivaretas også på områder som faller utenfor vårt tilsynsområde.

Datatilsynet har en rekke virkemidler til disposisjon for å løse oppgavene:

- **Tilsyn og saksbehandling** brukes for å avdekke brudd på regelverket og pålegge endringer. I tillegg til å korrigere enkeltvirksomheters behandling av personopplysninger, bidrar dette ofte til endret praksis i hele sektoren.

- **Veiledning, fortolkning og rådgivning** om regelverket er et annet og viktig virkemiddel. Vi mottar hvert år hundrevis klager fra enkeltpersoner som opplever at personvernet deres krenkes. Vi kommer også med en lang rekke uttalelser om hvordan regelverket skal tolkes og forstås, og vi gir råd til mange tusen enkeltpersoner, bedrifter, organisasjoner og offentlige organer. Dette bidrar til større forståelse for regelverket og forebygger senere klagesaker.

- Datatilsynet driver også med **utstrakt utredningsarbeid**, og publiserer årlig rapporter om dagsaktuelle personvernutfordringer – særlig knyttet til teknologiske trender. Disse rapportene har fått stor oppmerksomhet både nasjonalt og internasjonalt, og bidrar til å påvirke ulike sektorer og opplyse hver enkelt om rettigheter og utfordringer for personvernet.

- I tillegg benytter vi **kommunikasjon** som et virkemiddel for å støtte opp under oppgavene våre. Vi holder foredrag, gir uttalelser og kommer med innspill til media, publiserer veiledninger og nettartikler på hjemmesiden, har egen blogg og bruker sosiale medier. I tillegg arrangerer vi seminar og lanserer kampanjer både på eget initiativ og i samarbeid med andre. Vi er også med på å drifte et undervisningsopplegg rettet mot barn og unge.

Med de nye personvernreglene får Datatilsynet nye virkemidler, borgerne nye rettigheter og virksomhetene nye plikter. Det nye regelverket legger opp til at den enkelte sektor selv tar ansvar for å følge regelverket.

De nye pliktene til å vurdere personvernkonsekvenser, følge prinsippene for innebygd personvern og forhåndsdrøfte behandlinger med høy risiko, vil underbygge ansvarlighetsprinsippet. Dette prinsippet understreker at det er virksomheten selv som gjennom sine rutiner, handlinger og sitt daglige arbeid er ansvarlig for å følge loven. Datatilsynets rolle som rådgiver og pådriver overfor den enkelte sektor og virksomhet, vil også styrkes med de nye reglene.

Våre verdier

Datatilsynets ansatte har sammen kommet frem til hvilke fire verdier vi skal jobbe etter og som skal prege måten tilsynet arbeider på.

Uredde

- Vi skal være en aktiv, modig og tydelig stemme i personverndebatten.
- Vi skal være en sterk forsvarer av individets integritet og frihet.

Fremtidsrettede

- Vi skal være nytenkende og sette tema med stor betydning for personvernet på dagsorden.
- Vi skal være tidlig ute med å identifisere trender og personverntrusler.

Troverdige

- Vi skal være lydhøre og møte andre med interesse, respekt og dialog.
- Vi skal være tydelige på når vi utøver vår forvaltningsrolle og når vi utøver vår ombudsrolle.
- Vi skal sørge for at våre avgjørelser, uttalelser og vurderinger er solid forankret i faglig kunnskap, dokumentert praksis og erfaring.

Kunnskapsrike

- Vi skal ha god kunnskap om ulike målgruppers behov og synspunkter.
- Vi skal ha en kultur som dyrker medarbeidernes nysgjerrighet, faglig utvikling og initiativ.

Hva er personvern?

Demokratiet, rettsstaten og menneskerettighetene er bygd opp basert på en aksept for at det enkelte menneske er myndig, selvstendig, ansvarlig og uavhengig. Begrepet personvern er tett knyttet til disse verdiene. For at vi mennesker skal kunne utvikle selvstendige refleksjoner og vurderinger, trenger vi en privat sfære som ikke er kontrollert av andre.

Samtidig er ikke retten til personvern absolutt. Et samfunn skal ivareta både frihet og trygghet for sine borgere. Mens friheten forutsetter vern av den private sfære, vil en inngripen i denne friheten ofte være en forutsetning for å skape trygghet. I likhet med andre menneskerettigheter må retten til privatliv balanseres mot andre hensyn, og i noen tilfeller må personvernhensyn vike for hensyn til sikkerhet, trygghet og åpenhet – for å nevne noe.

Personvernet som menneskerettighet og overordnet verdi er nedfelt i Den europeiske menneskerettskonvensjonen (EMK) og i Grunnloven hvor personvernet kommer til uttrykk som en rett til privatliv:

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.» (EMK artikkel 8)

«Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin kommunikasjon. Husransakelse må ikke finne sted, unntatt i kriminelle tilfeller.
Statens myndigheter skal sikre et vern om den personlige integritet.»
(Grunnloven §102)

I EU/EØS-retten (personverndirektivet (95/46/EC) og personopplysningsloven med forskrift) kommer plikter og rettigheter knyttet til personvern først og fremst til uttrykk som regler om personopplysningsvern eller «data protection». Dette er fordi personvern i praksis i stor grad handler om enkeltmenneskets rett til å ha innflytelse på bruk og spredning av personopplysninger om seg selv.

I forarbeidene til personopplysningsloven (NOU 1997: 19, kapittel 3) forsøkes det å klargjøre personvernbegrepet ved at det ses fra ulike synsvinkler; nemlig det integritetsfokuserte, det maktfokuserte og det beslutningsfokuserte personvernet.

- Fra den integritetsfokuserte synsvinkel har vi alle et grunnleggende ønske om å ha kontroll over opplysninger om oss selv, og særlig gjelder dette opplysninger som oppleves som personlige og intime.

- Fra den maktfokuserte synsvinkel kan personvern forklares med utgangspunkt i at «kunnskap er makt» og at kunnskap om andre mennesker gir makt. Ut ifra et slikt ståsted kan det være viktig å motvirke at noen styrker sin posisjon ved å ha tilgang til mye og betydningsfull personinformasjon.

- Fra den beslutningsfokuserte synsvinkel er det et viktig premiss at personopplysninger brukes som grunnlag for beslutninger, og at det derfor er viktig for oss at opplysninger som brukes er relevante og korrekte.

Alle disse sidene av personvernbegrepet gjenspeiles i de nye personvernreglene. Særlig kommer de til uttrykk gjennom de grunnleggende prinsippene for behandling av personopplysninger.

Grunnleggende prinsipper for vern av personopplysninger

Reglene for behandling av personopplysninger bygger på noen grunnleggende prinsipper som er beskrevet i personvernforordningens artikkel fem. Alle som behandler personopplysninger må opptre i samsvar med disse prinsippene.

Lovlig, rettferdig og gjennomsiktig

At behandlingen av personopplysninger må være **lovlig**, innebærer først og fremst at det må finnes et rettslig grunnlag for en planlagt behandling av personopplysninger. Personvernforordningen har en liste over rettslige grunnlag, og minst ett av disse må være oppfylt. Prinsippet om lovlighet kan også sies å inkludere alle de øvrige prinsippene og reglene for behandling av personopplysninger som en behandlingsansvarlig må oppfylle.

At behandlingen av personopplysninger må skje **rettferdig** betyr at den skal gjøres i respekt for de registrertes interesser og rimelige forventninger. Behandlingen skal være forståelig for de registrerte og ikke foregå på skjulte eller manipulerende måter.

Gjennomsiktig betyr at bruken av personopplysninger skal være oversiktlig og forutsigbar for den opplysningene gjelder. Gjennomsiktighet bidrar til å skape tillit og setter enkeltpersonen i stand til å bruke sine rettigheter og ivareta sine interesser.

Formålsbegrensning

Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og være forklart på en måte som gjør at alle berørte har samme forståelse av hva opplysningene skal brukes til.

For at formålet skal være legitimt må det i tillegg ha et rettslig grunnlag som er i samsvar med etiske og rettslige samfunnsnormer. Personopplysninger kan ikke gjenbrukes til formål som er uforenelig med det opprinnelige formålet.

Dataminimering

Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen. Dersom personopplysningene ikke er nødvendige for å oppnå formålet, skal man heller ikke samle dem inn.

Riktighet

Personopplysninger som behandles skal være korrekte, og skal om nødvendig oppdateres. Dette betyr at den behandlingsansvarlige må sørge for å straks slette eller rette personopplysninger som er uriktige.

Lagringsbegrensning

Prinsippet om lagringsbegrensning innebærer at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.

Integritet, konfidensialitet og tilgjengelighet

Personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet og tilgjengelighet beskyttes. Dette betyr at den behandlingsansvarlige må sørge for tiltak mot utilsiktet og ulovlig ødeleggelse, tap og endringer av personopplysninger.

Ansvarlighet

Prinsippet om ansvarlighet understreker ansvaret for å opptre i samsvar med prinsippene for behandling av personopplysninger og for å ivareta de registrertes rettigheter og friheter. Dette ansvaret ligger på alle virksomheter som behandler

personopplysninger. Det er ikke nok å bare **ha** ansvar – man må vise at man **tar** ansvar.

Dette betyr at virksomheten må kunne dokumentere at den har gjennomført tiltak for å etterleve personvernforordningen. Virksomheten må opptre proaktivt og etablere nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.

Omverdensanalyse – personvern er viktigere enn noensinne

Oljen har i flere tiår vært driveren i norsk økonomi. Oljeplattformen har vært symbolet på norsk velstand. Denne er nå sakte, men sikkert i ferd med å bli erstattet med et annet symbol, dataskyen. I det 20. århundret var oljen det viktigste premisset for vekst og endring. I det 21. århundret spiller derimot data en helt avgjørende rolle i utviklingen av norsk økonomi og samfunn.

Personopplysninger er byggesteinene i det nye datadrevne samfunnet. Det er enorme muligheter knyttet til denne utviklingen, men det intensiverer også bruken av folk sine opplysninger i en helt annen skala enn vi har sett tidligere.

Norge digitaliseres, automatiseres og personaliseres

De siste 20–30 årene har Norge gjennomgått en omfattende digitalisering. Digitaliseringen berører alle sektorer, inkludert handel med varer og tjenester, offentlig sektor, skole og ikke minst den private sfære. I de siste årene har vi også sett at utviklingen går i retning av mer personaliserte tjenester, og at stadig flere beslutninger automatiseres og overlates til maskiner. Følgende er sentrale elementer som har bidratt til denne utviklingen:

- **Stordata.** Digitaliseringen av samfunnet har generert store mengder personopplysninger som ved hjelp av avanserte algoritmer kan gi detaljerte analyser av hver enkelt av oss.

- **Tingenes internett.** Sensorer og datamaskiner integrert i produkter som smartklokker, strømmålere og husholdningsprodukter bidrar til produksjon av stordata. I dag finnes det over 10 milliarder gjenstander som er tilknyttet internett, innen 2020 vil dette mangedobles.

- **Lagring- og analysekapasitet.** I 2017 koster datalagring en tidel av hva det gjorde for ti år siden og skytjenester gjør at man kan få enkel og billig tilgang til lagring og analysekapasitet.

- **Kunstig intelligens.** Bedre analyse av data gjennom algoritmer, maskinlæring og kunstig intelligens gjør at data som før ikke ga verdi eller

mening for seg selv, kan settes sammen i en ny kontekst finne mønstre og gjøre analyser om enkeltpersoner med ekstrem nøyaktighet.

- **Infrastruktur og deling**. Plattformer gjør det enklere å dele og bruke data på tvers. For eksempel innen helsesektoren er det pågående prosesser for å samle og tilgjengeliggjøre data i plattformstrukturer til forskjellige formål, som pasientjournaler, innbyggertjenester eller forskning.

- **Forventinger til bruk av data.** Nordmenn er blitt vant til digitaliserte tjenester, og forventer i økende grad at tjenestene skal være personaliserte. Både kommersielle og offentlige tjenestetilbydere står overfor brukere som ønsker enkle, brukervennlige tjenester som er skreddersydd deres behov.

Data er makt

Personopplysninger er en viktig ressurs, og tilgang til opplysningene gir innsikt i og kunnskap om folks liv, vaner, interesser og behov. Denne kunnskapen påvirker maktbalansen i samfunnet.

Data er makt i politiske valg, men også på det økonomiske markedet. Store kommersielle aktører sitter på enorme mengder data om alle. De har en tilsvarende stor konkurransefordel når det kommer til utvikling av intelligent teknologi og det å kunne tilby de mest personaliserte og presise tjenestene. Denne konkurransefordelen skaper utfordringer for mindre aktører som ikke klarer å konkurrere, og som kanskje ender opp med å kjøpe teknologi, data eller analysetjenester fra gigantene. Dette resulterer i færre valgmuligheter for forbrukerne. Små og alternative tjenester blir skviset ut av markedet, noen av dem med potensielt bedre personvernvilkår enn de store selskapene.

Markedsdominansen til noen få globale selskap skaper også dilemmaer for norsk offentlig sektor som må ta stilling til om de skal kjøpe tjenestene til disse selskapene. På den ene siden tilbyr selskapene de mest avanserte og effektive verktøyene, men på den andre siden kan myndighetene miste nasjonal suverenitet over egne systemer og data.

Borgerne eller forbrukerne har frem til nå vært den svake part både i møte med kommersielle og offentlige aktører fordi de i stor grad har måttet godta de vilkårene som blir tilbudt. Med sterkere rettigheter i et nytt felleseuropeisk personvernregelverk er det et potensial for et skifte i maktbalansen som regulerer tilgang og eierskap til data – i favør forbrukeren.

Personvern vs. kriminalitet

Personvern er en grunnleggende menneskerettighet. Noen ganger kommer denne rettigheten i konflikt med motstridende hensyn. Siden terrorangrepene i USA i 2001 har vi sett en rekke personverninngripende tiltak i Norge i regi av staten. Tiltakene har hatt som mål å forebygge eller bekjempe kriminalitet, terror eller internettrelaterte trusler.

Da datalagringsdirektivet ble vedtatt i 2011, åpnet Stortinget for føre-var-innsamling av data om alle norske borgere. Vedtaket ble senere kjent ugyldig av EU-domstolen, blant annet fordi lagring kan føre til at folk får en følelse av å være under konstant overvåking.

I 2016 fikk politiet tilgang til å bruke dataavlesing ved etterforskning, avverging og forebygging av alvorlig kriminalitet. Dette er et integritetskrenkende inngrep som er et stykke på vei til å kriminalisere tanken. Samme år ble også et forslag om å innføre et digitalt grenseforsvar lagt fram. Dette vil innebære overvåking av kommunikasjonen til de fleste innbyggerne i Norge, uten hensyn til om de har vært involvert i en straffbar handling eller ikke.

Dette er eksempler på tiltak som innebærer inngrep i personvernet til den enkelte innbygger. Økt lagrings- og prosesseringskapasitet, samt bruk av kunstig intelligens, muliggjør større omfang og dybde på overvåkingstiltakene, og er noe som vil utfordre personvernet også i årene fremover.

Trusselen fra den virtuelle verden

Internettrelatert kriminalitet øker i omfang verden over. Norge er et av verdens mest digitaliserte land og våre personopplysninger er dermed spesielt utsatt. Datatrusler kan komme i mange ulike former, alt fra dataspionasje til propagandakampanjer og «kidnapping» av data.

Vi ser at både offentlig og privat sektor tar i bruk gode og billige IT-løsninger fra utlandet i stort omfang. Samtidig erfarer vi at kompetansen på sårbarhets- og risikovurderinger ikke er tilfredsstillende. Konsekvensen av mangelfulle risikovurderinger gjør virksomhetene sårbare for innbrudd og lekkasjer av data.

Tradisjonelt har internettrelatert kriminalitet først og fremst gått etter mål av sikkerhetspolitisk interesse, slik som for eksempel store virksomheter, politikere, forsvar og medier. Men også blant vanlige norske virksomheter og innbyggere er datakriminalitet et problem.

I mange datatrusselsituasjoner er det konfidensialiteten eller integriteten til opplysningene som blir brutt, altså at opplysningene kan bli manipulert eller komme i feil hender. Men vi ser også at blokkering av tilgang til opplysninger kan skape store samfunnsmessige og personlige utfordringer.

Hva betyr mer overvåking og intensiv bruk av data for personvernet?

Mengden data om oss som er i omløp, er i økning. Det skaper muligheter for mer presise og tilrettelagte tjenester. Mer data gjør det også mulig å overvåke og spore livene våre i detalj. Hvilken betydning har dette for personvernet vårt?

- **Nedkjølingseffekt**. Vissheten om at alle data vi legger igjen kan fanges opp og potensielt ha en konsekvens i fremtiden, kan påvirke hvordan folk lever livene sine. Man kan tenke seg at noen vil unnlate å gjøre eller si ting som vil kunne slå dårlig ut.

- **Tap av kontroll over egne opplysninger.** Dagens digitale borger ferdes i et landskap der man ikke har full oversikt over hvilke spor man legger igjen, hvem som har tilgang til personopplysningene og hva konsekvensene av at data blir lagt igjen kan være. Dette utfordrer kjernen av personvernet som innebærer at hver enkelt skal ha kontroll over hvem som har tilgang til ens personopplysninger og hvordan de brukes.

- **Ugjennomsiktige algoritmer.** Både i privat og offentlig sektor automatiseres ulike tjenester. Algoritmene som gjør vurderingene, blir mer og mer avanserte og samtidig vanskeligere å forstå. Transparens og åpenhet rundt automatiserte vurderinger er avgjørende for å sikre at brukeren har kontroll på egne opplysninger og kan bruke sine rettigheter.

- **Sporing som standard.** I takt med at flere og flere av tjenestene som tilbys baserer seg på sporing og personalisering, ser vi en fare for at alternativene for de som ønsker å benytte en anonym tjeneste blir få eller ikke-eksisterende. Det er en fare for at sporingsfrie alternativer blir dyrere eller upraktiske – noe som vil presse folk til å oppgi personopplysningene sine selv om de egentlig ikke ønsker det.

- **Diskriminering og sosial ulikhet.** Algoritmer baserer seg ofte på data man allerede har om enkeltpersoner eller grupper. Disse kan i enkelte tilfeller være preget av fordommer og skjevheter. Algoritmene kan også diskriminere enten som en del av programmeringen, eller fordi dataene som brukes dytter analysen eller beslutningen i en bestemt retning.

Nytt regelverk, nye løsninger

I løpet av virkeperioden til denne strategien ser vi at reglene for bruk av personopplysninger skjerpes og oppdateres til å være mer tilpasset dagens teknologi. Det nye regelverket innebærer som tidligere nevnt større ansvar på virksomheten selv til å etterleve reglene (ansvarlighetsprinsippet), og styrker personvernrettighetene til folk flest.

Sanksjonsmulighetene til Datatilsynet blir også styrket, noe som betyr potensielt større konsekvenser ved overtredelser av regelverket.

Det nye regelverket bidrar til et større fokus på personvern. En av nyvinningene med det nye regelverket er at alle system og løsninger må bygge inn personvernet fra start – såkalt innebygd personvern. Dette er en forutsetning for godt personvern, og et viktig tiltak for å sikre at systemet oppfyller rettighetene de registrerte har og at virksomheten møter kravene i regelverket.

I 2018 blir sannsynligvis også reguleringen av e-privacy fra EU implementert. Denne har som mål å styrke personvernet i elektronisk kommunikasjon, og har blant annet krav til anonymisering, lagring og sletting av innhold og metadata i elektronisk kommunikasjon på nett. Reglene vil også gi den registrerte mer kontroll over egne opplysninger ved å gjøre det lettere å samtykke eller å ikke samtykke til bruk av informasjonskapsler.

Begge disse regelverkene gjelder i alle EU- og EØS-land og er en del av en europeisk harmoniseringsstrategi for bruk av data. Dataflyten krysser grenser, og vi i Datatilsynet er nødt til å jobbe på tvers av grenser for å ivareta personvernrettighetene på best mulig måte – også når det gjelder land utenfor Europa.

Personvern under press

Personvernet er under press og i endring. Ny teknologi slik som kunstig intelligens, stordata og forventingene til folk flest bidrar til et mer og mer dataintensivt samfunn. De etablerte personvernprinsippene, slik som at det skal foreligge et

bestemt formål for å behandle data, at det ikke skal behandles mer data enn nødvendig og åpenhet rundt bruk av data, utfordres.

Som ressurser, har oljen og persondata noe til felles. Begge bidrar til velstand og fremgang, men bruken kan ha negative konsekvenser. Et interessant fellestrekk mellom global oppvarming og et svekket personvern, er at begge ofte ikke er et umiddelbart problem der og da, men heller problemer som vil materialisere seg på lang sikt. Problemene kan derfor oppleves som fjerne og vanskelig å forholde seg til for mange. Oljesøl og personopplysninger på avveier kan også selvfølgelig være umiddelbare problemer, men den store utfordringen kommer på lang sikt.

Når det kommer til bruken av personopplysninger som en grunnleggende ressurs for å sikre vekst og velstand i samfunnet, er samfunnet avhengig av at borgerne har tillit til at opplysningene om dem blir håndtert på en sikker og rettferdig måte. Hvis folk ikke har tillit, vil de være mer forsiktige med å dele opplysningene sine. Konsekvensen kan enten være dårligere data, dårligere tilgang på data eller at dataene blir brukt mot deres vilje – noe som er en utfordring for demokratiet og samfunnet som helhet.

Målet for denne treårsstrategien er å bidra til en god balanse mellom ulike ønsker; det å kunne bruke personopplysninger til ulike formål for å oppnå gevinst for det offentlige, næringslivet og den enkelte på den ene siden, og å gjøre dette på en måte som ivaretar personvernet til hver enkelt, på den andre.

Strategiske mål

Datatilsynet har lovpålagte kjerneoppgaver som innebærer saksbehandling, veiledning, tilsyns- og kommunikasjonsvirksomhet. For å oppnå best mulig personvern, er vi nødt til å prioritere oppgavene og jobbe strategisk. Vi har derfor utarbeidet seks strategiske mål som skal være styrende for Datatilsynets arbeid i tre år fra og med januar 2018.

1. Datatilsynet skal arbeide for en mer rettferdig maktbalanse mellom individet på den ene siden, og kommersielle aktører og det offentlige på den andre.

Store kommersielle selskap og offentlige myndigheter sitter på store mengder data om enkeltindivider. For hvert enkelt individ er det vanskelig å ha kontroll over egne opplysninger. Datatilsynet vil jobbe målrettet for å styrke personvernprinsippene og -rettighetene til den enkelte.

Vi skal

- prioritere prinsippsaker som kan bidra til å endre maktbalansen i favør av enkeltpersoner
- aktivt håndheve regelverket for å sikre bedre etterlevelse blant aktører som har en forretningsmodell som utfordrer personvernet i særlig grad
- samarbeide med andre tilsyn og relevante organisasjoner for å styrke den enkeltes rettigheter nasjonalt og internasjonalt
- aktivt påvirke politiske prosesser og lovgivningsarbeid som legger føringer for bruken av personopplysninger i privat og offentlig sektor
- aktivt delta i debatten om overvåking i samfunnet, og verne om viktige prinsipper i Den europeiske menneskerettskonvensjonen og Grunnloven

2. Datatilsynet skal arbeide for å fremme personvernvennlig digitalisering, innovasjon og utvikling.

Bruk av stordata kan bidra til å løse en rekke av utfordringene samfunnet står overfor. Samtidig utfordrer bruken av stordata grunnleggende personvernrettigheter. Å lage løsninger som muliggjør utnyttelse av store datamengder, samtidig som personvernulempene for enkeltindividet reduseres mest mulig, vil bli enda viktigere fremover.

Vi skal

- ansvarliggjøre dataintensive aktører til å utvikle og ta i bruk metoder som ivaretar personvernet på en god måte
- arbeide for at relevante myndigheter setter av mer midler til forskning på personvernfremmende teknologi
- fremme bruk av innebygd personvern og håndheve brudd ved manglende etterlevelse
- bidra til å øke kompetansen om personvernkonsekvensvurderinger
- jobbe for at personvern er en del av bestillingskompetansen i offentlig og privat sektor
- jobbe aktivt for at universitet og høgskoler innarbeider personvern i alle relevante utdanninger

3. Datatilsynet skal arbeide for at virksomheter blir kompetente, forstår viktigheten av godt personvern og etterlever regelverket.

Det nye personvernregelverket legger mer av ansvaret for å ivareta personvernet på en god måte over på virksomhetene. For å kunne ta dette ansvaret og etterleve regelverket, er virksomhetene avhengige av å ha tilstrekkelig kompetanse. De må forstå hvorfor og hvordan personvern er viktig for både virksomheten selv og enkeltpersonene de har opplysninger om.

Vi skal

- synliggjøre personvern som verdi for virksomhetene
- aktivt bruke samarbeidspartnere til å sikre god kompetanse og etterlevelse i ulike sektorer
- påvirke sentrale aktører til å ta ansvar for at det arbeides med personvern i sektorer tilpasset sektorens behov
- oppfordre til utvikling og bruk av selvregulerende mekanismer slik som bransjenormer, standardisering og sertifisering
- gi god veiledning og gode verktøy som hjelper virksomhetene å etterleve regelverket
- sørge for at virksomhetene ivaretar rettighetene til de registrerte og åpner for enkel klagetilgang
- sørge for at virksomheter som har plikt til det oppretter personvernombud og at disse ombudene har god kompetanse og rolleforståelse

4. Datatilsynet skal bidra til at individet i større grad kan ivareta sitt eget personvern.

Opplysninger om enkeltpersoner er en ressurs som kan utnyttes, og for å beskytte seg selv er det viktig at hver enkelt lett kan finne informasjon om rettighetene sine og selv kunne utøve dem i praksis.

Vi skal

- synliggjøre verdien av personvern for den enkelte og samfunnet som helhet
- utvikle veiledningsmateriell og selvhjelpsverktøy for å hjelpe enkeltpersoner til å ivareta rettighetene sine
- påvirke virksomheter og bransjer til å utvikle gode løsninger som hjelper enkeltpersoner til å ivareta rettighetene sine
- jobbe for å styrke opplæringen om personvern og digital kompetanse i skolen

5. Datatilsynet skal påvirke og ta lederrollen i noen utvalgte internasjonale prosesser for å fremme bedre personvern.

Mange personvernrelevante prosesser og beslutninger som påvirker norske innbyggere blir tatt internasjonalt. Personvernforordningen krever at tilsynsmyndighetene samarbeider om saker på tvers av grenser. Det er derfor viktig at det norske Datatilsynet tar en aktiv rolle i det internasjonale arbeidet.

Vi skal

- aktivt delta i europeiske og internasjonale forum og prosjekter for å påvirke beslutninger og praktisering av regelverket som påvirker personvernet til norske borgere
- ta en pådriverrolle i det nordiske samarbeidet
- bruke vårt nasjonale arbeid (veiledninger, utredninger, avgjørelser) til å skape merverdi internasjonalt
- hente kompetanse og lære fra det som skjer internasjonalt

6. Datatilsynet skal være et kompetent og fremtidsrettet tilsyn.

Datatilsynet skal være en kunnskapsbasert arbeidsplass med stor takhøyde og godt arbeidsmiljø.

Vi skal

- være en aktiv, modig og tydelig stemme i personverndebatten
- være i forkant av samfunnsmessige og teknologiske trender som har betydning for personvernet
- samarbeide med relevante forskningsmiljøer og drive eget analysearbeid for å sette fokus på viktige utviklingstrekk som påvirker personvernet
- bygge opp god forståelse av nasjonale og europeiske beslutningsprosesser
- sørge for at medarbeiderne i Datatilsynet har kompetansen de trenger for å utføre oppgavene sine på best mulig måte
- ha åpne arbeidsprosesser med stor mulighet til å påvirke egen arbeidshverdag
- jobbe for å ha en mest mulig strømlinjeformet organisasjon, god ressursplanlegging og effektiv saksbehandling

Besøksadresse:
Tollbugata 3, 0152 Oslo

Postadresse:
Postboks 8177 Dep.,
0034 Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no