DATATILSYNETS STRATEGI

2021 - 2023

Datatilsynet

Innhold

Om strategien

Personvernlandskapet er i stadig endring, og det er viktig at vi i Datatilsynet jobber langsiktig og strategisk, holder oss oppdatert på teknologitrender og sørger for å være godt synlige. I denne strategien har vi definert 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.

Denne strategien trer i kraft tre år etter at et nytt personvernregelverk (GDPR) ble implementert i Europa i 2018. Samtidig står vi i 2021 midt oppe i en verdensomspennende pandemi. Parallelt opplever vi at bruken av personopplysninger intensiveres både i offentlig og privat sektor. Utviklingen mot det datadrevne samfunn åpner opp for enorme muligheter, men også store farer. Hvorvidt vi makter å treffe den riktige balansen mellom mulighetene og farene, vil bli avgjørende for hvilket samfunn vi skaper sammen.

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

Vi har hentet inspirasjon internt og eksternt i utviklingen av strategien. Vi har gjennomført både samlinger og internt gruppearbeid der vi har identifisert muligheter og utfordringer for personvernet generelt og for tilsynet spesielt. Dette har dannet utgangspunktet for arbeidet.

På bakgrunn av erfaringene våre med innkomne saker og henvendelser, diverse kunnskapsgrunnlag nasjonalt og internasjonalt og den offentlige debatten, har vi utarbeidet en omverdensanalyse som har vært med på å danne grunnlag for de strategiske målene.

Datatilsynet – roller og virkemidler

Med personvernforordningen har Datatilsynet fått gode virkemidler, borgerne tydeligere rettigheter og virksomhetene nye plikter.

Regelverket legger opp til at den enkelte sektor selv tar ansvar for å følge regelverket. Pliktene til å vurdere personvernkonsekvenser følger prinsippene for innebygd personvern og underbygger 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, er styrket med personvernforordningen.

Datatilsynets viktigste oppgave er å føre tilsyn med blant annet personopplysningsloven og personvernforordningen, 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 vi skal jobbe for at personvernet ivaretas også på områder som faller utenfor vårt tilsynsområde.

Datatilsynet har flere virkemidler til disposisjon for å løse oppgavene:

Tilsyn og saksbehandling. Gjennom saksbehandlingen tilegner vi oss erfaring og kunnskap om hvordan personvernhensyn ivaretas i praksis, og vi skal særlig ha oppmerksomheten rettet mot å identifisere systemfeil i virksomheter og bransjer. Saksbehandling som virkemiddel har særlig vært brukt på områder der vi mottar mange henvendelser og klager. Etter at personvernforordningen kom, har vi blant annet mottatt flere tusen avviksmeldinger fra virksomheter landet rundt. I tillegg til å korrigere enkeltvirksomheters behandling av personopplysninger, bidrar dette ofte til endret praksis i hele sektoren.

Tilsynsvirksomheten gir oss et faktabasert grunnlag for kommunikasjon til ulike bransjer og relevante aktører. Tilsyn kan benyttes aktivt for å undersøke og avklare praksis, og til å følge opp konkrete problemstillinger i enkeltsaker. Andre ganger

kan kontrollene benyttes til å få bedre oversikt over et område eller en sektor, og for å skaffe et bedre grunnlag for å ta i bruk de andre virkemidlene.

Kommunikasjon og veiledning. Datatilsynet skal veilede og informere om personvernlovgivning og forvaltningspraksis. Kommunikasjon som virkemiddel benyttes ofte sammen med de øvrige virkemidlene. En del av kommunikasjonen og dialogen vår skjer derfor gjennom veiledningstjenesten, veiledningsmøter og annen dialog med rammesettere, beslutningstakere, virksomheter og enkeltpersoner.

Gjennom kommunikasjon ønsker vi dessuten å spre informasjon om personvernets tilstand, samt skape debatt og gi uttrykk for synspunkter vi måtte ha som forvaltnings- og tilsynsorgan og i rollen som ombud. Ombudsrollen brukes blant annet ved utspill og kommentarer overfor mediene, i foredragsvirksomheten og i blogginnlegg.

Forsknings-, utviklings- og utredningsarbeid. Gjennom nær kontakt med miljøer i inn- og utland som driver med forsknings- og utviklingsarbeid, setter vi oss selv bedre i stand til å sette personvernhensyn inn i en samfunnsmessig kontekst, og til å fange opp trender og utviklingstrekk på et tidlig stadium. Vår kontakt med forskningsmiljøer kan stimulere til forskning på personvern, samtidig som personvernhensyn også blir ivaretatt i annen forskning.

Vårt eget utrednings- og kartleggingsarbeid utgjør også en viktig kilde til kunnskap. Det gir dybde til ulike temaer vi jobber med og er med på å skape oppmerksomhet om personvernspørsmål.

Regulatorisk sandkasse. Vi opprettet en regulatorisk sandkasse for kunstig intelligens i 2020. Her tilbyr vi kvalifisert veiledning til et utvalgt antall virksomheter. Målet med sandkassen er å stimulere til utvikling av innovative og samfunnsnyttige tjenester med godt, innebygd personvern. Sandkassen vil hjelpe virksomhetene til å følge regelverket, og samtidig bidra til kompetansebygging både hos den enkelte virksomhet og innad i Datatilsynet.

Andre virkemidler. Deltagelse i ulike råd og utvalg er et godt virkemiddel for å best mulig kunne påvirke aktører til å etablere god praksis. Det samme gjelder deltagelse i arbeid knyttet til innebygd personvern og regelverksutvikling. En slik måte å arbeide på egner seg særlig på områder der det pågår større reformer og utviklingsarbeid, særlig dersom de er teknologidrevne.

Våre verdier

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

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)

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 person-opplysninger. 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 behandlings-ansvarlige 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

Forbrenningsmotoren, oljeplattformen og månelandingsfartøyet kan på ulike måter fungere som symboler på menneskelig fremskritt, utvikling og vekst de siste århundrene. Når oljealderen gradvis nærmer seg slutten, trer imidlertid dataskyen frem som det definerende symbolet på vekst, fremskritt og makt. Byggesteinene i den digitale økonomien er i stor grad personopplysninger.

Utviklingen mot det datadrevne samfunn åpner opp for enorme muligheter, men også store farer. Hvorvidt vi makter å treffe den riktige balansen mellom mulighetene og farene, vil bli avgjørende for hvilket samfunn vi skaper sammen.

Data er makt

Data, i mange tilfeller personopplysninger, er i økende grad den viktigste forutsetningen for å lykkes i dette stadig mer datadrevne samfunnet. Det gjelder både for private og offentlige aktører. Tilgang til opplysninger om folks liv, vaner, handlinger, bevegelsesmønster, nettverk og tanker kan i økende grad oversettes til en form for råvare som det er mulig å profittere på. Det kan gjøres ved å tilby de beste, mest personaliserte tjenestene. Datafangst gir i tillegg et stort konkurransefortrinn i kappløpet om å utvikle kunstig intelligens.

Store, kommersielle aktører samler inn enorme mengder data om alle som tar i bruk tjenestene deres, og nettverkseffekter forsterker et knippe amerikanske og kinesiske selskapers globale dominans i den digitale økonomien. Mindre aktører blir skviset i dette markedet, ender opp med dårligere tilgang på data og blir ofte tvunget til å kjøpe tjenester av de globale gigantene. Resultatet for enkeltindividet blir færre valgmuligheter og at aktører med potensielt bedre personvernvilkår ikke overlever.

Den økende erkjennelsen av makten som ligger i storstilt datafangst, og potensialet de samme dataene representerer for positiv samfunnsutvikling, skaper utfordringer for offentlige myndigheter. I takt med den teknologiske utviklingen har forventningene til bedre og mer personaliserte tjenester økt. Ulike aktører og fagmiljøer presser på for å få tilgang til offentlige data for å utvikle tjenester som kan komme befolkningen til gode.

Offentlig forvaltning samler rutinemessig inn store mengder personopplysninger om samtlige innbyggere. Opplysningene inkluderer svært sensitiv informasjon, som for eksempel helseopplysninger. Slik sett er staten en viktig maktfaktor når det gjelder persondata, og de enorme digitaliseringsprosjektene innen helsesektoren vitner om et høyt ambisjonsnivå når det gjelder å trekke verdier ut av dataene. Samtidig bidrar slike store digitaliseringsprosjekter til økt sårbarhet for sikkerhetsbrudd som følge av angrep mot IT-løsninger og infrastruktur.

Større, raskere, mer

Vi står på terskelen av virkelig store gjennombrudd når det gjelder kunstig intelligens. Brukt riktig kan slik teknologi bidra til positiv samfunnsutvikling innen en rekke ulike sektorer, som blant annet samferdsel, medisin, energi og velferdstjenester. Sannsynligvis må vi lene oss på samme teknologi hvis vi skal lykkes med å snu den eskalerende klimakrisen. Stadig flere selskap og offentlige aktører tar i bruk systemer som helt eller delvis er basert på slik teknologi.

Samtidig er den samme teknologien et sentralt undertrykkingsverktøy i noen av verdens mest totalitære overvåkingssamfunn. For eksempel er kunstig intelligens en sentral komponent i ansiktsgjenkjenningsteknologi, som i økende grad integreres i moderne kameraovervåkingssystemer. I tillegg blir autonome våpensystemer brukt i væpnede konflikter og cyberkrigføring blir en større og viktigere del av de militære stormaktenes våpenarsenal.

Parallelt med utviklingen av kunstig intelligens skjer det et taktskifte i utbredelsen av sensorer og kameraer integrert i produkter vi omgås og interagerer med til vanlig, det såkalte tingenes internett. Smartklokker som registrerer biometriske data, kjøleskap som holder orden på matvarenes datostempling, strømmålere som kontinuerlig registrerer forbruk og automatisk justerer temperatur, stemmestyrte assistenter og smarte hus og byer blir mer og mer utbredt. Slike produkter har en åpenbar forbrukerverdi, men utgjør like åpenbart en risiko for den enkeltes personvern.

Når produktene vi omgir oss med er koblet til internett, følger en økt risiko for å miste kontroll over personopplysningene som registreres, det være seg til selskapene som leverer produktene eller ondsinnede aktører. Utbredelsen av femte generasjons trådløst internett, 5G-nettet, vil også ha en eskalerende effekt på de overnevnte utviklingstrekkene. Når dette tas i full bruk, vil det føre til et kraftig dytt i internettilkoblede sensorers mulighet til å behandle og utveksle data. Et slikt taktskifte vil også ha konsekvenser for den enkeltes personvern.

Økende motstand mot teknogigantene

De mest verdifulle selskapene på nittenhundretallet var oljeselskap. I dag topper et knippe amerikanske og kinesiske teknologiselskaper den samme listen. Tilgangen til data, samt kapasitet og kompetanse til å trekke verdier ut av store mengder data, er den viktigste grunnen til disse selskapenes dominans.

Samtidig leverer disse selskapene sentrale komponenter i den digitale infrastrukturen som moderne samfunn er helt avhengige av. Sentrale norske institusjoner bruker for eksempel i dag skytjenester levert av amerikanske selskap til datalagring og drift av systemer. Det innebærer at vi har skapt et avhengighetsforhold som det kan bli vanskelig å fri seg fra. Flere og flere ytrer skepsis mot at vi lar privateide, utenlandske selskap stå som garantister for at det digitale Norge holder seg flytende.

Sosiale medier har i praksis utkonkurrert tradisjonelle medier som den viktigste offentlighetssfæren i store deler av verden. Mange går til Facebook for å oppdatere seg på nyheter, politikk og samfunn. Norske politikere, partier, pressgrupper og organisasjoner som søker samfunnsendring, migrerer også over til Facebook og andre sosiale medier. Dermed kan de omgå de redaktørstyrte medienes portvokterfunksjon i sin jakt på velgere, påvirkning og makt. Det betyr at vi har fått en algoritmisk styrt offentlighet, der informasjonen den enkelte eksponeres for, styres av eksisterende nettverk og klikkhistorikk. Dette skjer samtidig som tradisjonelle nyhetsmedier årelates, fordi annonseinntektene følger den samme migrasjonen over til Facebook. Følgene av denne utviklingen er en relativisering av sannheten, økt polarisering og en mindre velfungerende demokratisk offentlighet.

Facebook og Apple konkurrerer om å bli markedsledende innen betalingstjenester, og Google satser tungt på helsesektoren. På samme måte som Google har monopolisert markedet for nettsøk, posisjonerer Amazon seg for å innta det skandinaviske varehandelsmarkedet og Uber jobber for å innta persontransportmarkedet. Lignende selskap med samme forretningsmodell vil etter all sannsynlighet se etter neste mulighet til å overta eksisterende markeder ved hjelp av sterk finansiell ryggdekning og avansert teknologi.

Personvern og kriminalitet

Personvern er en grunnleggende rettighet, men må samtidig veies opp mot andre til dels motstridende hensyn slik som sikkerhet. Siden årtusenskiftet har kriminalitets- og terrorbekjempelse i økende grad fått forrang for personvern i

mange vestlige land, en forskyvning som særlig ble forsterket av terrorangrepene mot USA i 2001.

I Norge har slike interessemotsetninger særlig manifestert seg i debatten om datalagringsdirektivet i 2011, et vedtak som senere ble kjent ugyldig av EU-domstolen. I 2016 fikk politiet tilgang til å bruke dataavlesing ved etterforskning, avverging og forebygging av alvorlig kriminalitet.

I 2019 la regjeringen frem et forslag om ny etterretningstjenestelov, som blant annet inneholdt to kapitler om det som ble kalt «tilrettelagt innhenting». Forslaget innebar at etterretningstjenesten ville få tilgang til både metadata og innhold i nett- og teletrafikken som går ut av Norge, noe som flytter grensen for overvåking av befolkningen dramatisk. Lovforslaget ble vedtatt i Stortinget til tross for store protester fra en rekke høyst ulike instanser og fagmiljøer. Rett før den skulle implementeres i 2021 ble kapitlene som omhandler masseinnsamling av datatrafikk utsatt, som følge av to dommer i EU-domstolen som slo fast at generell og udifferensiert innsamling av teledata i bulk er i strid med kommunikasjonsvernsdirektivet.

Eksemplene viser at balansegangen mellom personvern og kriminalitetsbekjempelse aldri er hugget i sten, men må gjøres ut fra konkrete vurderinger av fordeler og ulemper for den enkelte og samfunnet som helhet. Sterke krefter med legitime agendaer vil alltid søke å forskyve balansen i retning av mer overvåking og flere kontrolltiltak. Når omfanget og dybden av hvilke typer opplysninger det er mulig å registrere øker i takt med lagrings- og prosesseringskapasiteten, øker også presset på enkeltindividets personvern. Hvor det riktige balansepunktet skal gå må konstant debatteres, også når terrorbekjempelse ligger i den andre vektskålen.

Cybertrusselen

Når samfunn digitaliseres, øker sårbarheten for datakriminalitet. Norge er ett av verdens mest digitaliserte land og norske borgeres personopplysninger er dermed spesielt utsatt. Cyberangrep kan være motivert av ren økonomisk vinning, for eksempel i form av ransomware, men slike angrep inngår også i stadig større grad som en del av staters våpenarsenal i geopolitiske konflikter. Omfanget av statlige og statsfinansierte aktørers angrep mot rivaliserende staters infrastruktur, næringsliv og økonomi, er i stor grad ukjent. Men når stadig større deler av en nasjons infrastruktur digitaliseres, øker den potensielle gevinsten for fiendtlige aktører.

Datakriminalitet kan ramme mål av økonomisk og sikkerhetspolitisk interesse, men også være politisk og aktivistisk motivert. I 2020 ble for eksempel Stortinget utsatt for et målrettet cyberangrep.

Også blant vanlige norske virksomheter og innbyggere er datakriminalitet et problem, og jevnlig avsløres det angrep mot norske mål. Ikke alle virksomheter har tilstrekkelig kompetanse til å håndtere den stadig økende mengden digitale trusler. Sårbarhets- og risikovurderinger er ikke alltid tilfredsstillende. Konsekvensene av mangelfulle risikovurderinger kan for eksempel være datalekkasjer, manipulering av datainnholdet eller økt nedetid for systemene.

At Norge er et sårbart land i møte med digitale trusler, bekreftes også av studier som viser at Norge har et økende underskudd på kompetanse innen informasjons-sikkerhet. Manglende etterlevelse av informasjonssikkerhetskravene i regelverkene vi forvalter, har vært grunnlag for flere av de største overtredelsesgebyrene Datatilsynet har utstedt de siste årene.

Koronapandemiens eskalerende effekt

Våren 2020 vil for alltid huskes som våren da verden stengte ned. Et nyoppdaget koronavirus sveipet over kloden og førte til at myndigheter over hele verden iverksatte kraftige tiltak for å stagge utbruddet. Norske myndigheters tiltak var de mest inngripende noen regjering har innført i fredstid, og vi ble nødt til å leve med sterke begrensninger på vår individuelle frihet i påvente av en effektiv vaksine.

Historien har imidlertid vist oss at ekstraordinære tiltak i krisesituasjoner ofte blir en ny normaltilstand. Det er derfor avgjørende at samfunnets grunnleggende demokratiske kontrollfunksjoner opprettholdes og følges også når trusselnivået endres. Koronaloven, som åpner for at regjeringen kan hasteinnføre tiltak for å respondere raskt nok på virustrusselen, bør for eksempel ha en begrenset virkeperiode.

Norske myndigheter nyter relativt stor tillit i befolkningen. Likevel har vi også her til lands sett noe motstand mot de mest inngripende tiltakene, selv om de massive protestene andre land har opplevd i stor grad har uteblitt.

Når samfunnet stengte ned åpnet det seg et vindu for hastedigitalisering av flere sektorer. En stor del av arbeidslivet ble over natten flyttet til hjemmekontor og barn måtte undervises på hjemmeskole. For arbeidstakere som fortsatte å møte på jobb, ble det innført nye og inngripende kontrollmekanismer, slik som krav om helse-erklæringer og temperaturmålinger. Arbeidsstokken på hjemmekontor møtte krav

om effektivitetsmålinger og andre kontrollmekanismer som ville vært utenkelige i en normaltilstand.

Skoleelever måtte på kort tid venne seg til en ny skolehverdag, med digital kommunikasjon og skolearbeid. Mange lærere ble tvunget til å ta i bruk digitale verktøy og programmer som de i liten grad var kjent med tidligere. I helsesektoren ble digitale pasientkonsultasjoner og digital kommunikasjon en ny normal omtrent over natten.

Den påtvungne hastedigitaliseringen av samfunnet i kjølvannet av nedstengingen har medført en økt risiko for befolkningens personvern i form av arbeidslivs-overvåking, men også ved at ondsinnede aktører, som hackere og svindlere, har benyttet sjansen til å utnytte sårbare mennesker i en usikker og konfliktfylt tid.

Pandemien førte også til at myndigheter over hele verden i raskt tempo utviklet løsninger for digital smittesporing. I Norge ble appen Smittestopp lansert, men ble etter pålegg av Datatilsynet trukket tilbake etter kort tid og etter en stund relansert i en ny og mer personvernvennlig versjon.

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 april 2021.

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. Vi vil jobbe målrettet for å styrke personvernprinsippene og -rettighetene til den enkelte, samt de demokratiske prinsippene som personvern er en forutsetning for.

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 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
- jobbe for en mer rettferdig maktbalanse mellom store, utenlandske teknologiselskaper og norske aktører
- kommunisere arbeidet vi gjør for å bedre maktbalansen i favør av enkelt-personer

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 personvern-rettigheter. Å lage løsninger som muliggjør utnyttelse av store datamengder, samtidig som personvernulempene reduseres mest mulig, vil bli enda viktigere fremover.

Vi skal

- drifte og videreutvikle en regulatorisk sandkasse for kunstig intelligens
- ansvarliggjøre dataintensive aktører til å utvikle og ta i bruk metoder som ivaretar personvernet på en god måte
- jobbe for at relevante myndigheter setter av mer midler til forskning på personvernfremmende teknologi
- fremme bruk av innebygd personvern og håndheve brudd ved manglende etterlevelse
- jobbe aktivt for at universitet og høgskoler innarbeider personvern i alle relevante utdanninger

3. Datatilsynet skal arbeide for at virksomheter har nødvendig kompetanse, forstår viktigheten av godt personvern og etterlever regelverket.

Ansvaret for å ivareta personvernet ligger hos virksomhetene som behandler personopplysninger. For å oppfylle regelverkets krav til ansvarlighet må virksomhetene ha vilje og evne til å prioritere kontinuerlig arbeid med å sikre etterlevelse i driften og ivareta de registrertes rettigheter. For å få til dette trenger virksomhetene kompetanse og ressurser, i tillegg til en grunnleggende forståelse av hvorfor personvern er en viktig verdi både for dem selv og enkeltpersonene de har opplysninger om.

Vi skal

- synliggjøre at personvern er et konkurransefortrinn, i tillegg til en nødvendighet
- aktivt bruke samarbeidspartnere i ulike sektorer og påvirke sentrale aktører til å sikre nødvendig kompetanse og etterlevelse
- oppfordre til utvikling og bruk av selvregulerende mekanismer slik som nasjonale retningslinjer, bransjenormer, standardiserings- og sertifiseringsløsninger
- gi veiledning og utarbeide verktøy som hjelper virksomhetene å etterleve regelverket
- bidra til å øke kompetansen om personvernkonsekvensvurderinger
- jobbe for at personvern er en del av bestillingskompetansen i offentlig og privat sektor, samt at personvernkrav blir en del av offisielle statlige dokumenter
- kontrollere at virksomhetene ivaretar rettighetene til de registrerte og at de sørger for enkel klagetilgang
- kontrollere at virksomheter som har plikt til det, oppretter personvern-ombud 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, og konsekvensene av dårlig ivaretatt personvern, for den enkelte og samfunnet som helhet
- snakke enhetlig og konsekvent i alle kanalene våre og i møte med samfunnet
- utvikle veiledningsmateriell, selvhjelpsverktøy og maler 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, samt knytte til oss eksterne ungdomsråd eller personvern-ambassadører i målgruppen

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

Mange personvernrelevante prosesser og beslutninger som påvirker norske innbyggere, blir tatt internasjonalt. Det er derfor viktig at vi tar en aktiv rolle i det internasjonale arbeidet.

Vi skal

- delta aktivt i europeiske og internasjonale forum og prosjekter for å påvirke beslutninger og praktisering av regelverket som påvirker personvernet til norske borgere
- bidra i det nordiske samarbeidet
- bruke det nasjonale arbeidet vårt, blant annet i form av veiledninger, utredninger og avgjørelser, til å skape merverdi internasjonalt
- hente kompetanse og lære fra det som skjer internasjonalt
- utveksle erfaringer og samarbeide med andre land, både om utvalgte problemstillinger og i konkrete saker

6. Datatilsynet skal være et kompetent, fleksibelt og fremtidsrettet tilsyn.

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

Vi skal

- være en aktiv, modig og tydelig stemme i personverndebatten
- sikre kontinuitet og samhold i en organisasjon som evner å snu seg raskt rundt i møte med nye utfordringer
- 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
- sørge for at medarbeiderne våre har kompetansen de trenger for å utføre oppgavene sine på best mulig måte
- ha åpne arbeidsprosesser med stor mulighet til å påvirke egen arbeids-hverdag
- jobbe for best mulig ressursplanlegging, grundige risikovurderinger og effektiv saksbehandling

Besøksadresse:
Trelastgata 3, 0152 Oslo

Postadresse:
Postboks 458 Sentrum
0105 Oslo

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

datatilsynet.no
personvernbloggen.no