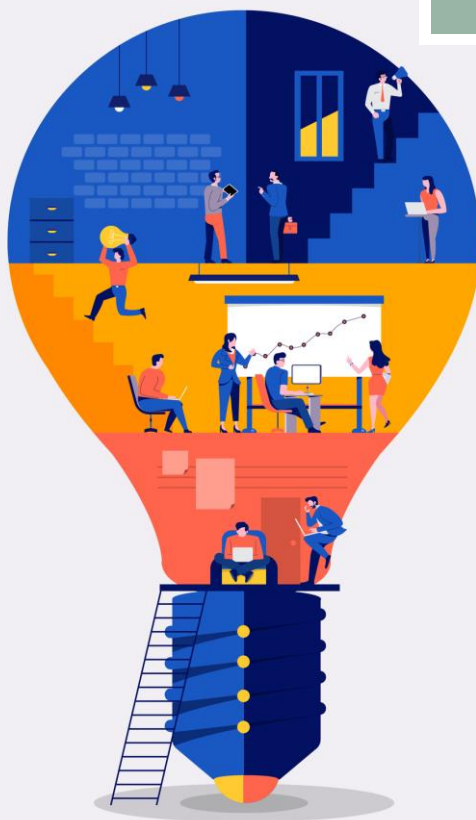




DATATILSYNETS STRATEGI

2024 - 2026



Datatilsynet

Innhold

Innledning	4
Innsatsområder	7
Datatilsynet – roller og verdier	10
Omverdensanalyse: En datadrevet og urolig verden.....	11

Innledning

Datatilsynet er et uavhengig forvaltningsorgan under Digitaliserings- og forvaltningsdepartementet (DFD). Hovedoppgaven vår er å bidra til at personvernlovgivningen etterlevs, og at alle skal ha beskyttelse i tråd med personopplysningsregelverket. Hovedmålet i samfunnsoppdraget vårt er **et godt personvern for alle**.

Vi skal fremme personvern som en sentral verdi i samfunnet, delta i personverndebatten og sette dagsorden i personvernspørsmål. Vi skal også undersøke og dele fakta om personvernets kår både nasjonalt og internasjonalt.

Datatilsynet skal bidra til ansvarlig digitalisering og bruk av personopplysninger i Norge. Målet med en overordnet strategi, er å peke ut en klar retning for arbeidet vårt for å kunne oppnå best mulig personvern for alle.

Vi har hentet inspirasjon internt og eksternt i utviklingen av strategien. Vi har fått innspill fra over 160 offentlige og private virksomheter om hvilke muligheter og utfordringer de ser for personvernområdet i årene fremover. Gjennom de over 5000 årlige henvendelsene vi får til veiledningstjenesten vår, samt klagesakene vi mottar fra enkeltpersoner, får vi også en god pekepinn på hva norske innbyggere er opptatt av og hvor personvernet er under mest press. Vi har dessuten gjennomført strategisamlinger der alle ansatte i tilsynet har vært med å stake ut veien videre.

Strategien er bygd rundt en overordnet visjon. I tillegg til visjonen har vi fire satsingsområder som utgjør «huset» og «grunnmuren» som visjonen er bygget på. Hvert satsingsområde har mål som vi skal operasjonalisere i tilsynets virksomhetsplan i hvert av de tre årene strategien gjelder.

Strategien inkluderer også en beskrivelse av Datatilsynets roller og verdier, og en omverdensanalyse som setter strategien i en samfunnskontekst.

Hva er personvern?

Personvern handler om retten til et privatliv og retten til å bestemme over egne personopplysninger. Du har rett på en privat sfære som du selv kontrollerer og hvor du kan handle fritt uten tvang eller innblanding fra staten eller andre mennesker.

Personvern er ikke bare en viktig menneskerettighet som skal sikre hensynet til den enkeltes personlige integritet og privatliv. Et dårlig ivaretatt personvern vil også sette demokratiet i fare ved at borgerne begrenser sin deltakelse i åpen meningsutveksling og politisk aktivitet.

Retten til personvern er nedfelt i Den europeiske menneskerettskonvensjonen (EMK) og i den norske Grunnloven.

I tillegg har vi personopplysningsloven og personvernforordningen som regulerer bruken av personopplysninger på tvers av sektorer, og uavhengig av hvilke verktøy eller teknologi som tas i bruk. Hovedformålet med dette regelverket er å ivareta fysiske personers rettigheter i forbindelse med behandling av personopplysninger, og å sikre fri utveksling av personopplysning i EU/EØS.

Regelverket inneholder både rettigheter og plikter. Det er bygd på noen grunnleggende prinsipper alle som behandler personopplysninger må opptre i samsvar med. Personvernprinsippene handler om:

- Lovlighet, rettferdighet og gjennomsiktighet
- Formålsbegrensing
- Dataminimering
- Riktighet
- Lagringsbegrensing
- Integritet og konfidensialitet
- Ansvarlighet

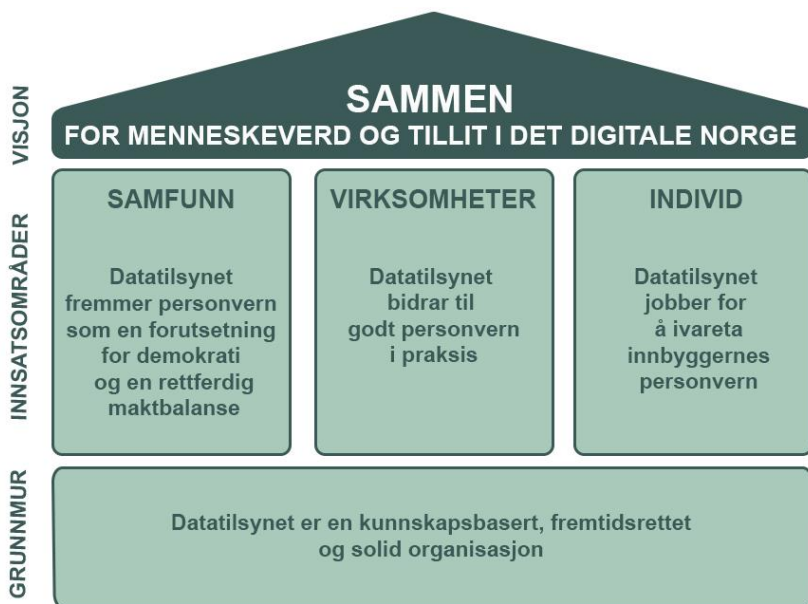
Visjon

Datatilsynets overordnede visjon er:

Sammen for menneskeverd og tillit i det digitale Norge

Det norske samfunnet er i en digital omstillingsprosess. Datatilsynet skal bidra til at personvernet til innbyggerne ivaretas i denne prosessen for å sikre en digitalisering som bevarer menneskeverdet og bygger tillit.

Visjonen starter med ordet «sammen». For å nå de strategiske målene, er det helt avgjørende for Datatilsynet å jobbe sammen med andre myndigheter, virksomheter, interesseorganisasjoner og innbyggerne. Også internt i tilsynet skal vi jobbe sammen på tvers av fag for å få til best mulig personvern for alle.



Innsatsområder

Datatilsynet har mange forskjellige lovpålagte kjerneoppgaver. For å oppnå best mulig personvern, er vi nødt til å prioritere oppgavene og jobbe strategisk. Vi har derfor kommet frem til fire innsatsområder som skal være styrende for Datatilsynets arbeid i strategiperioden.

Innsatsområde 1: Samfunn

Datatilsynet skal fremme personvern som en forutsetning for demokrati og en rettferdig maktbalanse

Delmål:

- Vi bidrar aktivt til rettferdig og personvernvennlig digitalisering og bruk av kunstig intelligens.
- Vi fremmer viktigheten av personvern som en menneskerettighet.
- Vi jobber for å motvirke manipulative forretningsmodeller, filterbobler og diskriminerende algoritmer, og vi fremmer personvern som grunnlag for et fritt ordskifte.
- Vi er en pådriver for en helhetlig personvernpolitikk og har en tydelig stemme i samfunnsdebatten.
- Vi jobber aktivt for å ivareta personvernet i politiske prosesser.
- Vi påvirker regelverksutvikling nasjonalt og internasjonalt.

Innsatsområde 2: Virksomheter

Datatilsynet skal bidra til godt personvern i praksis

Delmål:

- Vi fremmer verdien av godt personvern for virksomhetene.
- Vi bidrar til at virksomheter har innebygd personvern i utviklingen og bruken av ny teknologi og nye løsninger.
- Vi prioriterer tiltak som gir stor effekt for personvernet til mange.
- Vi jobber målrettet for å nå bredt ut med praktisk veiledning.
- Vi har godt samarbeid og dialog med relevante aktører for å få til godt personvern i ulike sektorer.

Innsatsområde 3: Individ

Datatilsynet skal jobbe for å ivareta innbyggernes personvern

Delmål:

- Vi bidrar til at enkeltindividet kjenner rettighetene sine og er i stand til å bruke dem ovenfor virksomhetene.
- Vi prioriterer tiltak som gir stor effekt for personvernet til mange.
- Vi jobber for å ivareta personvernet til sårbare og utsatte grupper.

Innsatsområde 4: Grunnmur

Datatilsynet skal være en kunnskapsbasert, fremtidsrettet og solid organisasjon

Delmål:

- Vi har god ressursstyring for å oppnå målene våre på en effektiv måte.
- Vi prøver ut nye metoder og arbeidsformer.
- Vi går foran som et godt eksempel ved å ivareta personvernet i de digitale hjelpemidlene vi selv benytter.
- Vi bygger kompetanse og jobber tverrfaglig.
- Vi er en virksomhet med klare rammer og gode arbeidsverktøy.
- Vi har et godt og inkluderende arbeidsmiljø.

Datatilsynet – roller og verdier

Datatilsynet har på den ene siden en reaktiv rolle hvor vi fører tilsyn og kan ilegge sanksjoner. Vi fører tilsyn med personopplysningsloven, politiregisterloven, kredittopplysningsloven, helseregisterloven, helseforskningsloven, pasientjournalloven og Lov om Schengen informasjonssystem. I tillegg har vi ansvar for tilsyn med forskrift om kameraovervåking i virksomhet og forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk utstyr.

På den andre siden har vi en proaktiv rolle hvor vi gir veiledning om hvordan etterleve regelverket, og vi deltar i det offentlige ordskiftet. Vi veileder myndigheter, virksomheter og enkeltpersoner i personvernspørsmål, vi deltar i personverndebatten, og vi undersøker og deler fakta om personvernets kår, både nasjonalt og internasjonalt.

Det er derfor viktig for oss at vi bruker virkemidlene våre på en effektiv og rettferdig måte, og at vi er tydelig på hvordan vi praktiserer rollene våre utad.

Verdier

Datatilsynets ansatte har kommet frem til tre verdier vi skal jobbe etter. Vi skal være:

1. **Uredde**
 - Vi er en aktiv, modig og tydelig stemme
 - Vi er lydhøre og møter andre med interesse og respekt
2. **Troverdige**
 - Vi er kunnskapsrike, etterrettelige og uavhengige
 - Vi jobber utadrettet, tverrfaglig og dialogbasert
3. **Fremtidsrettede**
 - Vi er nytenkende og setter tema med stor betydning for personvernet på dagsorden
 - Vi er i forkant og jobber strategisk

Omverdensanalyse: En datadrevet og urolig verden

Vi vil her identifisere noen tendenser som vi mener vil påvirke personvernet i årene fremover. Dette er en del av bakteppet for utformingen av strategien.

En urolig verden

De siste årene har vi opplevd en global pandemi og krig på europeisk jord. Andelen av verdens befolkning som lever i fullverdige demokratier er på tilbakegang, og autoritære ledere vinner eller tar makten i stadig flere land. Det digitale trusselbildet er i endring, og personopplysninger brukes blant annet i storskala cyberoperasjoner, i manipulering av innhold i digitale kanaler og til bruk i inngripende overvåking.

Historien har gang på gang vist oss at grunnleggende rettigheter ofres når en krise inntreffer. Terroren som traff verden 11. september 2001, er et eksempel på en hendelse som førte til omfattende og inngripende systemer og lover for overvåking. Koronapandemien utløste en lang rekke inngripende tiltak som begrenset menneskers frihet, og den stadig tilbakevendende terrortrusselen flytter grenser for hvor inngripende overvåkingsmetoder politi og etterretning ønsker å ta i bruk. Å forstå verdien av, og å kunne ivareta, personvern for menneskets og samfunnets integritet, blir enda viktigere i en urolig verden.

Kunstig intelligens overalt

Det har dessuten skjedd et taktskifte innen utviklingen av kunstig intelligens (KI). I det øyeblikket OpenAI lanserte ChatGPT, akselererte tempoet i KI-kappløpet mellom kommersielle selskap og mellom nasjoner. KI har lenge vært en komponent i forbrukerteknologi og har sakte, men sikkert, også gjort sitt inntog i offentlig forvaltning. I de årene denne strategien gjelder for, forventer vi at KI vil bli brukt aktivt i alle sektorer. Bruken vil bli mer avansert og inngripende enn det vi har sett tidligere.

De nyeste KI-anvendelsene er eid, finansiert og kontrollert av godt kjente selskap. Microsoft, Alphabet, Meta og de andre teknologikjempene kontrollerer en stadig større del av den grunnleggende digitale infrastruktur med forretningsmodeller som aktivt sporer livene våre, og omgjør data til profitt. Når KI integreres i enda flere tjenester og verktøy, vil sannsynligvis denne dynamikken forsterkes.

Store dominerende aktører skaper et ujevnt maktforhold mellom tilbydere og de som tar i bruk teknologien. En annen utfordring, er at KI i årene fremover vil kunne forsterke eksisterende forskjeller i samfunnet hvis beslutningstakere ikke tar aktive grep for å sikre en menneskevennlig og rettferdig bruk av teknologien. Algoritmer som lærer av et skjevt datagrunnlag, kan videreføre og forsterke skjevheter i samfunnet, og sårbare grupper og individer kan bli enda mer sårbare i møte med svarte bokser som tar avgjørelser som påvirker livene deres.

Reguleringsbølge fra EU

Personvernforordningen endret spillereglene for det digitale livet i Europa. I løpet av levetiden til denne strategien kommer flere EU-forordninger, inkludert Digital Services Act, Digital Markets Act, Digital Governance Act, AI Act og Data Act, til å bli gjeldende i Norge. Reguleringsbølgen fra EU er utformet for å temme teknologigigantenes innflytelse og legge til rette for ansvarlig digitalisering og innovasjon.

EU legger altså viktige premisser for digitalisering og bruk av data. Lovgivningstrenden går mot mer datadeling. Et interessant spørsmål i årene som kommer, er hvilken innvirkning dette vil ha på personvernforordningen og personvernet på sikt.

Norge er del av et europeisk marked, og vår praksis skal være harmonisert med resten av Europa. Det er viktig at Norge følger opp reguleringer og strategier fra EU. Samtidig er det viktig å sørge for at utviklingen skjer i praksis og i tråd med ønsker og behov i det norske samfunnet.

Muligheter og utfordringer fra virksomhetenes perspektiv

Våren 2023 fikk vi innspill fra over 160 offentlige og private virksomheter og organisasjoner om hvilke muligheter og utfordringer de ser for personvernområdet i årene som kommer. Kunstig intelligens var temaet som ble desidert mest hyppig nevnt. Men også andre teknologier slik som tingenes internett, blokk-kjeder, skytjenester, velferdsteknologi og generell digitalisering av samfunnet ble trukket frem.

Det var enighet om at personvern vil bli enda viktigere fremover fordi behandlingen av personopplysninger er sentralt i alle deler av samfunnet. Samtidig som virksomhetene så store muligheter med ny teknologi, så de også større sårbarheter og risikoer, for eksempel at data kommer på avveie som et resultat av hacking eller feil i IT-systemer.

Virksomhetene pekte også på en økende kompleksitet, både når det kommer til regelverk, teknologi og hvordan alt dette påvirker mennesker. Flere viste til at store globale aktører dominerer mye av teknologien og løsningene også i tiden fremover. Det er vanskelig for norske brukere og virksomheter å forstå hvordan opplysningene blir brukt og ha kontroll over egne data. I tillegg kommer geopolitiske utfordringer med leverandører fra land som kan ha interesse av å bruke data til etterretning eller manipulasjon.

Myndighetsovervåking er fortsatt en utfordring

Personvern har tradisjonelt handlet om å beskytte enkeltindividet fra myndigheters overvåking og kontroll. Uten frihet fra overvåking kan ikke frie samfunn eksistere. De siste årene har kommersiell overvåking og teknologikjempenes makt fått stadig større oppmerksomhet, men den samme teknologien er også svært interessant for offentlige myndigheter.

Flere konkrete lover og enkeltsaker illustrerer det offentliges ønsker og ambisjoner i et datadrevet samfunn. For eksempel har etterretningstjenestene fått utvidet fullmakt til å drive såkalt bulkinnnsamling av data som krysser landegrensene, politiet har fått utvidet adgang til å spore IP-adresser og PST til å samle inn informasjon fra åpne kilder. Lovene har møtt sterk motstand fra ulike fagmiljøer som beskytter grunnleggende rettigheter og demokratiet, og de vil sannsynligvis bli utfordret i norske og europeiske domstoler i tiden fremover.

Demokratisk nedkjøling

Personvern som konsept og lovene som regulerer personvernet, er i stor grad individfokusert. Fundamentalt sett handler det om beskyttelse av individets rett til frihet fra uforholdsmessig overvåking, manipulering og kontroll. Personvern har imidlertid også en kollektiv dimensjon som blir stadig viktigere jo mer digitale liv vi lever. Personvern er en forutsetning for andre verdier og rettigheter slik som ytringsfrihet, tankefrihet og demokrati.

Det økende omfanget av overvåking og registrering fra både kommersielle selskap og myndigheter, gjør at vi i noen tilfeller legge bånd på oss og er mer forsiktige enn vi ellers ville vært. Dette blir ofte omtalt som «nedkjølingseffekt». Individuelle personverninngrep kan i sum skape kollektiv skade ved at vi vegrer oss fra å søke informasjon, ta i bruk tjenester eller delta i samfunnsdebatten. Dette utfordrer demokratiske verdier som ytringsfrihet og retten til å søke informasjon, og det kan hindre folk å få tilgang til tjenester de har rett på.



Besøksadresse:

Trelastgata 3, 0152 Oslo

Postadresse:

Postboks 458 Sentrum

0105 Oslo

postkasse@datatilsynet.no

Telefon: +47 22 39 69 00

datatilsynet.no

personvernbloggen.no