Høringssvar – NOU 2022: 11 Ditt personvern – vårt felles ansvar. Personvernkommisjonens rapport.

Vi viser til brev av 11. november 2022 om høring på NOU 2022: 11 Ditt personvern – vårt felles ansvar. Personvernkommisjons rapport. Utredningen har vært på høring i Akademikernes medlemsorganisasjoner og vært behandlet i Akademikernes styre 6. februar 2023.

Akademikerne har noen generelle kommentarer knyttet personvern og koblingene mellom personvern og teknologi som diskuteres i utredningen, samt kommentarer knyttet til de konkrete forslagene til en nasjonal personvernpolitikk.

Generelle kommentarer

Retten til personvern er en menneskerettighet forankret i Den europeiske menneskerettighetskonvensjonen artikkel 8, «Enhver har rett til respekt for sitt privatliv og familieliv, sitt hjem og sin korrespondanse.», og fra 2014 i Grunnloven § 102,

> 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 myndighet skal sikre et vern om den personlige integritet.

Retten til personvern er en individuell rettighet, men samtidig en nødvendighet for et fungerende liberalt demokrati. Retten til personvern må også ses i sammenheng med den grunnlovfestede retten til ytringsfrihet. Uten personvern sammen med ytringsfrihet vil det for journalister ikke være mulig å opprettholde kildevernet, og uten retten til respekt for sin kommunikasjon vil det ikke være mulig å ha et sivilsamfunn utenfor staten eller for opposisjonspolitikere å drive politisk virksomhet.

En gjennomgående problemstilling er utfordringer knyttet til summen av lovlig innsamlet informasjon både i offentlig og privat sektor og mulige konsekvenser av dette. Ingen har i dag full oversikt over hvilke aktører som sitter på hvilken informasjon om det enkelte individ. Som utredningen viser kan store private aktører gjennom sammenstilling av forbruks- og adferdsdata utlede personsensitive opplysninger om deg, som så potensielt kan brukes på krenkende eller skadelidende måter. I en NATO-rapport referert i utredningen «advares det om at datameglerindustrien utgjør en trussel for nasjonal sikkerhet, på grunn av mengden informasjon

som samles inn om enkeltindivider». For staten vil kryssing av offentlige registre kunne gi full oversikt over enkeltindividets sårbare punkter.

Personvern i offentlig sektor

Den teknologiske utviklingen er verdinøytral, og bruken av kunstig intelligens sammen med systematisk innsamling av informasjon på individnivå vil gjøre det mulig for staten å levere velferdstjenester mer effektivt og med et mye større presisjonsnivå enn i dag. Imidlertid vil den samme informasjonen, enten ønsket eller utilsiktet, kunne brukes til å gradvis innskrenke borgernes frihet. For eksempel vil SSBs forslag om innsamling av transaksjonsdata sammenkoblet til Nav-data om sykefravær og personlig helseinformasjon teoretisk gjøre det mulig for staten å observere sammenhenger på personnivå mellom sykefravær, livsstilssykdommer og personlig konsumpsjon av f.eks. sukker, tobakk eller alkohol. Vi viser her til Akademikernes høringssvar til forslag for nasjonalt program for offisiell statistikk for perioden 2024-2027. I en tid med strammere offentlige budsjetter og større press på sykelønnsordningen og andre offentlige velferdsgoder vil man kunne se for seg at rett til eller nivå på offentlige ytelser kan kobles til individets valg i dagliglivet.

Hovedproblemet med det offentliges innsamling av personvernopplysninger er ikke den enkelte innsamlingen til det ene spesifikke formålet, men summen over tid og hva helheten kan brukes til. Samtidig som den enkelte innsamling og den enkelte sammenstilling er gjort for å kunne levere bedre offentlige tjenester og bedre utforme offentlig politikk vil særlig det offentliges mulighet, forutsatt at det gis lovhjemmel, til å sammenstille, ha innsyn i og benytte helheten av informasjonen kunne utgjøre en trussel mot individets personvern. Dette gjelder særlig for offentlige myndigheter som gjennom sine handlinger og fravær av handlinger kan påføre enkeltmennesker alvorlige konsekvenser, som for eksempel Nav, barnevern og politiet.

I kapittel 7.4.7.1 Håndtering av digitale beslag og overskuddsinformasjon skriver kommisjonen at de

> gjennom dialog med nøkkelpersoner i politiet også fått opplyst at manglende mulighet til å filtrere bort overskuddsinformasjon ved beslag av digitale lagringsenheter, utgjør en særlig risiko for de registrertes personvern. Når politiet beslaglegger en digital enhet, som for eksempel en datamaskin eller en mobiltelefon, vil det ofte også følge med informasjon som ikke er relevant for saken. Det finnes i dag ikke tekniske muligheter/verktøy for å filtrere bort slik overskuddsinformasjon. Det finnes heller ikke en spesialisert enhet som har myndighet til å gjennomgå og filtrere bort åpenbart irrelevante personopplysninger. Konsekvensen av at det per i dag ikke foreligger tekniske muligheter til å filtrere ut overskuddsinformasjon, eller en spesialisert enhet som har som oppgave å trekke ut informasjon uten betydning, er at mengder av personopplysninger som ikke er relevant for saken blir tatt vare på, og gjort tilgjengelig for mange.

Akademikerne mener at både innen justissektoren og ellers i offentlig sektor må prinsippet om dataminimering, altså at mengden personopplysninger som hentes inn og behandles begrenses til kun det som er nødvendig for å oppnå formålet, legges til grunn. Dette er nødvendig for å forhindre den form for formålsutglidning, særlig knyttet til overskuddsinformasjon, slik kommisjonen viser til i eksempelet over.

Det er nødvendig at personvern ses i sammenheng med ytringsfrihet. For vide hjemler for innsamling og behandling av offentlig tilgjengelig informasjon eller innhenting og lagring av metadata vil kunne gi nedkjølingseffekter på ytringsfriheten, som må unngås. Utfordringer med formålsglidning utover det personvernreglene tillater, vil også lett kunne oppstå når datamateriale samles inn og kombineres på nye måter. Dette er forhold som kan bidra til å uthule det individuelle rettsvernet.

Av Personvernkommisjonens mandat fremkommer det at den skulle

> kartlegge offentlig sektors behandling av personopplysninger til andre formål enn innsamlingsformålet, og gi en vurdering av de negative personvernkonsekvensene ved dette sett opp mot fordelene

Denne problematikken er særlig relevant for helseopplysninger, og må sees i sammenheng med risikoen for «nedkjøling», forstått slik at innbyggerne endrer atferd fordi de føler seg overvåket. Tillit til at helseopplysninger brukes i tråd med formålet for innhenting oppleves å være avgjørende for at pasienter skal avgi opplysninger til helsetjenesten. En nasjonal personvernpolitikk må vurdere i hvilken grad dette hensynet blir tilstrekkelig vektlagt ved forslag til etablering av ulike helseregistre og ved etablering av løsning for analyser av helsedata.

Det pågående arbeidet med å innlemme opplysninger om pasienter i den private tannhelsetjenesten i Kommunalt pasient- og brukerregister (KPR) kan stå som eksempel på at personvernhensyn ikke er tilstrekkelig vektlagt. Her gjennomføres en endring i forskriftsform med store personvernmessige konsekvenser, med henvisning til at Stortinget tok stilling til spørsmålet i 2016 og at det derfor ikke er nødvendig å utrede konsekvensene eller forelegge saken for Stortinget. Imidlertid var forutsetningen den gang at dersom det senere skulle bli aktuelt å innlemme flere opplysninger i KPR, skulle forslaget ut på en bred høringsrunde. Personvernutfordringer ble ikke diskutert da det ble foreslått en utvidelse av forskriften, og vurderingen av personvernkonsekvenser ble produsert nesten et år senere etter oppfordring fra Den norske tannlegeforening og Datatilsynet. I vurderingen ble så kravet om at det skal være *nødvendig* å samle inn opplysningene erstattet med at det er *nyttig.*

Kommentarer til personvernkommisjonens forslag

Forslagene til en nasjonal personvernpolitikk med tilhørende tiltak er presentert kronologisk og gruppert sammen der det er hensiktsmessig, med Akademikernes kommentarer etter forslagene. Ikke alle forslagene er direkte kommentert.

- En nasjonal personvernpolitikk må ha som overordnet mål å sørge for reell ivaretakelse av personvernet.
    - føre-var-prinsippet anvendes i tilfeller hvor teknologianvendelse innebærer særlig høy risiko for personvernet.
- En nasjonal personvernpolitikk må se personvernet i et helhetlig perspektiv.
    - Regjeringen årlig bør legge frem en personvernpolitisk redegjørelse for Stortinget, forankret i gjeldende personvernpolitikk.

En nasjonal personvernpolitikk vil kunne gi en helhetlig tilnærming til personvernproblemstillinger, og gi en bredere diskusjon enn en rent teknisk eller juridisk. Utviklingen av en nasjonal personvernpolitikk må sees i sammenheng med den teknologiske utviklingen. Samtidig må politikken være i stand til å knesette allmenngyldige og teknologinøytrale prinsipper for styrking og bevaring av personvernet. Det samme må være utgangspunktet for personvern-relevant lovgivning.

Teknologi er i seg selv nøytral, det er vi mennesker som bestemmer hvordan vi velger å sette den sammen og hva vi velger å bruke den til. Yrker som krever stor grad av kvalitative vurderinger som grunnlag for beslutninger vil kunne få stor hjelp av beslutningsstøttesystemer til å finne og vurdere relevant informasjon, hente og vurdere mot sammenlignbare saker og til å sikre et faglig sterkest og riktigst mulig beslutningsgrunnlag. Samtidig er systemene avhengige av informasjonen de får til å jobbe med, og kriteriesettene som styrer deres adferd. Som utredningen viser i eksempelet med den nederlandske skattemyndigheten kan et system bygget på gale premisser, som for eksempel ikke skiller mellom statistisk overrepresentasjon og individuell vurdering, gå på bekostning av rettssikkerheten.

I en liberal rettsstat må individets krav på rettssikkerhet gå foran muligheten for effektivitetsgevinster, både i privat og offentlig sektor. Akademikerne mener derfor at et generelt føre-var-prinsipp, der ny teknologi innføres med varsomhet på områder med personvernrelaterte problemstillinger, er hensiktsmessig og fornuftig særlig når den teknologiske utviklingen utvikles raskere enn regelverket.

I utviklingen av regelverket må lovgiver ta høyde for at lovgivningen ikke vil kunne holde følge med den teknologiske utviklingen. Akademikerne mener derfor at lovgivningen må være overordnet, prinsipiell og teknologinøytral, mens vurderinger og presiseringer knyttet til konkrete problemstillinger og teknologier må reguleres på lavere nivå. Videre er det nødvendig

å sikre at det ikke alene legges opp til juridiske barrierer for innsamling og benyttelse av personopplysninger, men også stilles krav til fysiske/tekniske barrierer.

Personvernet må også ivaretas i sammenhenger hvor det skal utvikles analysealgoritmer, for eksempel i forbindelse med maskinlæring og utvikling av kunstig intelligens. Her trenger utviklerne tilgang til rådata, altså store mengder personopplysninger som teknologien kan øve seg på, og det er viktig å sikre at opplysningene ikke kan kobles på en slik måte at enkeltpersoner kan identifiseres. Akademikerne mener det er nødvendig at denne problemstillingen ivaretas i en nasjonal personvernpolitikk.

I utformingen av regelverket er det nødvendig å se på regelverkets brukervennlighet opp mot hvem som faktisk vil være brukerne. Når teknologer lager tekniske løsninger, må de kunne forstå hvilket handlingsrom og hvilke sperrer jussen setter i utviklingen av algoritmene. De juridiske avgrensningene er særlig en utfordring der teknologi er utviklet utenfor EØS-området og det må foretas en vurdering av om teknologien er GDPR-kompatibel.

Også på brukernivå er det behov for at regelverket er forståelig. Dette er spesielt viktig i offentlig tjenesteyting hvor tilgang til og vurdering av sensitive personopplysninger er nødvendig for å kunne gi riktige tjenester.

- En nasjonal personvernpolitikk må innebære grundige risikovurderinger.

Etter Akademikernes syn er den største trusselen mot personvernet muligheten for formålsutgliding og myndighetsmisbruk. Som flere av eksemplene fra rapporten viser vil alle som har befatning med Nav, Skatteetaten eller andre offentlige myndigheter potensielt være sårbare grupper i møte med beslutninger eller vurderinger tatt på svakt eller feilaktig grunnlag. En nasjonal personvernpolitikk bør derfor rette særlig oppmerksomhet mot aktører som er så store og mektige at alle andre blir sårbare, herunder særskilt staten og offentlig sektor.

- En nasjonal personvernpolitikk må ha særlig oppmerksomhet på sårbare grupper, herunder barn og unge.
    - regjeringen arbeider for et forbud mot atferdsbasert markedsføring rettet mot barn. Skole- og barnehagesektoren må gå foran for å etterstrebe at personvernet ivaretas. Det er uakseptabelt at barns personopplysninger blir gjenstand for kommersiell utnyttelse.

Akademikerne mener det gjennomgående bør stilles strengere krav til det offentliges innsamling og bruk av personopplysninger. Videre bør privat næringsliv ha anledning til å drive næringsutvikling med utgangspunkt i bruk av personopplysninger på en annen måte enn det offentlige (Se under En nasjonal personvernpolitikk må fremme personvernvennlig innovasjon). Samtidig må det legges til grunn at kommersielle aktører ikke vederlagsfritt skal ha tilgang til offentlig innsamlede datasett av potensielt stor verdi.

For private leverandører av tjenester til det offentlige der borgerne ikke har reell mulighet til å velge vekk leverandøren uten at det går ut over deres tilgang på den samme offentlige tjenesten, må det stilles krav til innsamling, lagring og behandling av personopplysninger tilsvarende det som stilles til det offentlige. Dette er særlig fremtredende med den innføringen av digitale hjelpemidler man har sett i skolen de siste årene.

I rapporten Personvern i skolen gjør KS rede for anskaffelsesrutinene og en eventuell vurdering av personvernkonsekvenser. Videre melder KS om at flere kommuner påpeker at manglende ressurser og kapasitet gjør at slike vurderinger trekker ut i tid, til etter at anskaffelsen er gjennomført.

Akademikerne anser derfor at det ikke kan legges til grunn at kommunalt ansatte involvert i anskaffelsen av IT-utstyr til skolene, inkludert lærerne som skal benytte dette i undervisningen, har tilstrekkelig kompetanse til å gjøre de nødvendige personvernvurderingene i prosessen.

- En nasjonal personvernpolitikk må inkludere en tydelig utenrikspolitisk rolle.
- En nasjonal personvernpolitikk må utnytte det nasjonale handlingsrommet for regulering.
    - Norske myndigheter må føre en aktiv nasjonal lovgivningspolitikk for å fremme personvern. Det bør alltid være en ambisjon å bruke det nasjonale handlingsrommet som EU-lovgivningen gir, både for å supplere de europeiske reglene, støtte opp under og for å styrke gjeldende EU-lovgivning som norske myndigheter ser som spesielt viktig. Eventuelt bør norske myndigheter vedta avvikende norske regler dersom det er adgang og tilstrekkelig grunn til det.

Problemstillinger i krysningspunktet mellom teknologisk utvikling og personvern har også en sikkerhetspolitisk dimensjon. Selv om EUs personvernforordning (GDPR) gjelder i Norge kan det ikke uten videre antas at regelverket tolkes likt eller respekteres av teknologi- og innholdsprodusenter utenfor Europa. I tillegg til å benytte det handlingsrommet EU-lovgivningen gir for nasjonal tilpasning bør en nasjonal personvernpolitikk ta inn over seg og gjøre rede for sikkerhetspolitiske risikoer knyttet til personvern og individuell, kommersiell og offentlig bruk av teknologi, teknologileverandører og -eiere. Akademikerne deler derfor kommisjonens vurdering om at en nasjonal personvernpolitikk må inkludere en tydelig utenrikspolitisk rolle og må utnytte det nasjonale handlingsrommet for regulering.

- En nasjonal personvernpolitikk må fremme personvernvennlig innovasjon.
    - det bør utvikles robuste standarder og normer for å tydeliggjøre hvordan innovasjon kan skje innenfor etiske og forsvarlige rammer. Den nasjonale personvernpolitikken bør også styrke forskning og utvikling på personvernfeltet, for å bidra til personvernvennlig innovasjon og digitalisering.

Samtidig som *føre-var-prinsippet* gir en sunn kritisk tilnærming til bruken av ny teknologi er det norske samfunnet både avhengig av og i stand til å ligge i forkant i implementeringen og bruken av teknologiske nyvinninger. Som en del av en nasjonal personvernpolitikk er Akademikerne derfor enige med Personvernkommisjonen i at

> det bør utvikles robuste standarder og normer for å tydeliggjøre hvordan innovasjon kan skje innenfor etiske og forsvarlige rammer. Den nasjonale personvernpolitikken bør også styrke forskning og utvikling på personvernfeltet, for å bidra til personvernvennlig innovasjon og digitalisering. Forskning på personvernfeltet vil kunne ha stor betydning for vår evne til å forstå de samlede konsekvensene av digitaliseringen for innbyggernes grunnleggende rettigheter og friheter.

Personvern i privat sektor

Det er nødvendig å trekke en tydeligere grense om personvern mellom offentlig og privat sektor. Til tross for omfanget av private aktørers innsamling kan de ikke, som staten, tvinge deg til å oppgi personopplysninger, de vil ofte ha konkurrenter som leverer tilsvarende tjenester, og de sitter ikke på maktmidler tilsvarende statens voldsmonopol som potensielt kan misbrukes til å krenke individets rettigheter.

Private aktører har innenfor lovens rammer mulighet til å bedrive forskning og utvikling for å utvikle og benytte ny teknologi til å levere nye varer og tjenester. Som kommisjonen påpeker,

> Personopplysninger brukes til å utvikle og tilpasse tjenester basert på enkeltpersoners eller gruppers behov. Samtidig brukes personopplysninger til å målrette markedsføring. Innsamling og bruk av personopplysninger er ikke i seg selv problematisk, og kan være en forutsetning for utvikling av mange gode forbrukertjenester. Det er likevel en forutsetning for ivaretakelse av forbrukernes personvern at innsamling og bruk av personopplysninger skjer på en åpen, rettferdig og forståelig måte, og ikke er mer omfattende enn nødvendig.

Samtidig må rommet for å dele informasjonen med tredjepartsaktører, særlig aktører utenfor GDPRs virkeområde, tydelig begrenses, og kundens innsyn i og mulighet for å få egne opplysninger slettet må være tydelig rettighetsfestet og tilgjengelig. Det er her verd å merke seg, som utredningen påpeker, at

> Fremveksten av forretningsmodeller basert på innsamling av personopplysninger har derfor blitt møtt med kritikk fra blant annet menneskerettighetsorganisasjoner, forbrukerorganisasjoner og akademikere. Amnesty International har for eksempel uttalt at forretningsmodellene til Alphabet og Meta utgjør en trussel for flere grunnleggende menneskerettigheter.

Akademikerne mener at det her ikke kan være tilstrekkelig at forbrukeren som en del av et samtykkeskjema gir sin tilslutning til vilkår med et omfang og en teknisk tilnærming som

forbrukeren ikke realistisk kan forventes å sette seg inn i, og som gjør at det i praksis er umulig å gi et informert samtykke.

Videre må forbrukerens handlefrihet være reell. Denne handlefriheten reduseres betydelig og systematisk gjennom flere former for markedssvikt. Oligopol- og monopoltilstanden i deler av markedet der Google, Meta og Apple kjøper opp konkurrenter, deler brukerdata på tvers av ervervede tjenester, legger til rette for innelåsningmekanismer for forbrukerne og dyrker naturlige monopol, utgjør en alvorlig trussel både mot forbrukernes rettigheter og mot det frie markedets mulighet til å utvikle ny og bedre teknologi. Det er viktig at både nasjonale og internasjonale konkurransemyndigheter fortsetter å bekjempe denne utviklingen.

Næringslivets behov for tilstrekkelig handlingsrom til å kunne utvikle nye tjenester må balanseres mot forbrukernes interesser. Selv om sistnevntes personvern utvilsomt må komme først og regelverket må være strengt nok til å hindre en skritt-for-skritt-uthuling kan ikke regelverket være så strengt at det hindrer all innovasjon. Denne avveiningen må inngå i en nasjonal personvernpolitikk, men samtidig er utfordringen av en art hvor det ikke er mulig å finne hensiktsmessige løsninger på nasjonalt nivå.

- En nasjonal personvernpolitikk må innebære at offentlig sektor går foran.
    - offentlig sektor bruker sin innkjøpsmakt for å stimulere til fremveksten av personvernvennlige produkter og tjenester. Det bør gis føringer om hvordan personvern bør vektes i anskaffelser.

Akademikerne deler kommisjonens vurdering her.

- En nasjonal personvernpolitikk forutsetter et solid kunnskaps- og kompetansegrunnlag.
    - offentlig sektor må prioritere å styrke personvernkompetansen blant sine ansatte. Personvernpolitikken må også inneholde tiltak som sørger for at innbyggerne får grunnleggende opplæring i personvern.
    - personvern blir en del av grunnskoleutdanningen, og at undervisning i personvern styrkes på alle nivå, inkludert høyere utdanning.

Den teknologiske utviklingen er altfor rask og altfor spesialisert til at den enkelte voksne borger skal kunne gjøre selvstendige vurderinger knyttet til konkrete virkemidler eller teknologier. Derfor er en overordnet prinsipiell tilnærming knyttet sammen med en føre-var-tankegang de viktigste bærebjelkene i et befolkningsbredt kunnskaps- og kompetansegrunnlag rundt personvern. Det mest sentrale verktøyet for å oppnå dette er skolen.

Dybdeforståelse, kritisk tenkning, og fagenes rolle som felles kunnskapsgrunnlag og som allmenndannende er også nøkkelen til en befolkning som evner å tenke prinsipielt og med en *føre-var*-tilnærming til problemstillinger rundt personvern.

- En nasjonal personvernpolitikk forutsetter åpenhet rundt behandling av personopplysninger.
- En nasjonal personvernpolitikk forutsetter effektiv håndheving.
    - Datatilsynet må ha ressurser til veiledning av aktører med behov for det. Siden personvern stadig omfatter flere og større områder, må tilsynet styrkes i tråd med disse faktiske behovene.
    - også andre tilsynsmyndigheter enn Datatilsynet bør veilede om personvernspørsmål som direkte er knyttet til deres myndighetsområde

Som innbyggere har vi rett på innsyn i vedtak som omfatter oss. Dette må også inkludere hvordan personopplysninger i saken har blitt innhentet, hvilke personopplysninger som har blitt innhentet, hvorfor de er relevante og hva som er hjemmelsgrunnlaget for innhentingen. Dette må også inkludere hvilke kriterier og hvilket vurderingsgrunnlag en kunstig intelligens har lagt til grunn der den har medvirket som beslutningsstøtte.

Datatilsynet er avhengig av å ha tilstrekkelig ressurser til å følge den teknologiske utviklingen og spredningen av problemstillinger knyttet til personvern til nye områder. Dette gjelder som tilsyn og ombud overfor både myndighetene og private aktører, og som norsk representant i samarbeid med andre europeiske og internasjonale personvernmyndigheter. Akademikerne deler derfor kommisjonens vurderinger om Datatilsynets rolle og behov for styrking.

Oppsummering

- Personvern er både en grunnleggende menneskerettighet og en forutsetning for et velfungerende liberalt demokrati.
- Hovedutfordringen er ikke knyttet til enkeltstående brudd på personvernreglene, men summen av lovlig innsamlet informasjon både i offentlig og privat sektor og mulige konsekvenser av dette.
- Summen over tid av det offentliges innsamling av personopplysninger og det offentliges mulighet til å sammenstille, ha innsyn i og benytte helheten av informasjonen vil kunne utgjøre en trussel mot individets personvern.
- Av hensyn til borgernes rettssikkerhet og individets rett til privatliv må prinsippet om dataminimering legges til grunn for myndighetenes innhenting av personopplysninger, og myndighetenes anledning til å krysskoble forskjellige informasjonskilder med opplysninger om enkeltpersoner må begrenses.
- Individets krav på rettssikkerhet må gå foran muligheten for effektivitetsgevinster. Et generelt føre-var-prinsipp er derfor hensiktsmessig og fornuftig særlig når den teknologiske utviklingen utvikles raskere enn regelverket.
- For private leverandører av tjenester til det offentlige der borgerne ikke har reell mulighet til å velge vekk leverandøren uten at det går ut over deres tilgang på den

samme offentlige tjenesten stilles krav til innsamling, lagring og behandling av personopplysninger tilsvarende det som stilles til det offentlige.

- Det bør utvikles robuste standarder og normer for å tydeliggjøre hvordan innovasjon kan skje innenfor etiske og forsvarlige rammer. Den nasjonale personvernpolitikken bør også styrke forskning og utvikling på personvernfeltet, for å bidra til personvernvennlig innovasjon og digitalisering.
- Forbrukernes handlefrihet må være reell. Konkurransemyndighetene må hindre dominerende aktører i å misbruke sin markedsmakt.