Elektronisk Forpost Norge
Medlem av EDRi, European Digital Rights

Kommunal- og distriktsdepartementet
Via departementets høringsportal

24. februar 2023

Høringssvar - NOU 2022: 11 - Ditt personvern – vårt felles ansvar

Elektronisk Forpost Norge (EFN) takker Personvernkommisjonen for en fyldig og ikke minst etterlengtet utredning i «Ditt personvern - vårt felles ansvar NOU 2022: 11». Vi takker likeledes for muligheten til å delta i denne høringen og dermed uttrykke våre begrunnede synspunkter.

Med vennlig hilsen

Per Inge Østmoen
Styremedlem EFN

Elektronisk Forpost Norge
Pb 27 Vålerenga, 0626 OSLO E-Post: horing@efn.no Tlf. 996 24 544

Elektronisk Forpost Norge

Høringsuttalelse fra EFN

Innhold

Innledning

Utredningen danner grunnlaget for den brede samfunnsdiskusjon som vil være nødvendig i vår samtid når vi skriver 2023, hvor presset fra en rekke teknologier som hver for seg og samlet skaper større personvernmessige utfordringer enn svært mange tenker over i det daglige. Et samfunn med mange og komplekse offentlige funksjoner må ivareta sektorer som spenner over alt fra helse- og sosialområdet, utdannelse, arbeidsliv, rettsvesen, politi og forsvar, utallige forvaltningsoppgaver fra naturforvaltning til selve statens økonomi med alt hva det innebærer. Det er uunngåelig og også en nødvendighet at de mange funksjonene i samfunnet omfatter innsamling, håndtering og i varierende utstrekning også lagring av persondata.

Når persondata samles inn og behandles med et stort antall ulike formål, oppstår personvernessige og i videste forstand rettssikkerhetsmessige og også menneskerettighetsrelaterte problemstillinger som i sin ytterste konsekvens kan utgjøre alvorlige utfordringer for så vel enkeltmenneskets og fellesskapets rettssikkerhet, rettigheter og den friheten som de fleste vil mene bør være en grunnpillar i ethvert demokrati.

Personvernkommisjonen har i sitt arbeid vist god situasjonsinnsikt i ovennevnte, noe vi er glade for.

En altfor omfattende innsamling av persondata, og ikke minst en altfor omfattende lagring av også formålsunødvendige og formålsoverflødige data, kan med stor sikkerhet lede til både umiddelbare misbruk, formålsglidninger og resulterende fremtidige misbruk og uforholdsmessige inngrep i menneskers og grupper av menneskers hverdag og privatliv.

Her spiller teknologi og bruk av teknologi en nøkkelrolle. Nærmere bestemt hvordan, hvor og på hvilke premisser teknologi skal brukes, og det sentrale spørsmålet om hvem som skal kontrollere teknologien og definere grensene for anvendelsesområder. EFN konstaterer at det synes å ligge i mennesker og samfunn en tilbøyelighet til å ville benytte teknologiske verktøy og muligheter ut fra en i stor grad ubevisst styrende forestilling om at dersom en teknologisk mulighet foreligger, må den også benyttes og dertil benyttes i så stort omfang og på så mange områder som det til enhver tid er mulig å applisere den.

Denne ofte uheldige tilbøyeligheten kan observeres både hos myndigheter verden over, og hos «vanlige» borgere som etter vårt skjønn ofte har altfor lett for å tilpasse seg og godta inngripen og

tiltak som både i lys av menneskerettslige, rettssikkerhetsmessige og rimelige demokratiske forventninger til frihetsgrad for borgerne burde bli kontant og kompromissløst avvist. EFNs grunnleggende syn på de ulike personvernutfordringene er derfor at den aller viktigste, og faktisk helt avgjørende faktoren i personvernproblematikkens omfattende kompleks er helt vanlige borgeres bevissthet. Vi konstaterer derfor at de verdier vi i det foregående har signalisert at vi ønsker å opprettholde, best og mest effektivt forsvares av en bevisst og kritisk befolkning som evner å stille kritiske spørsmål ved både politiske maktstrukturers og myndigheters samt også andre andre aktørers disposisjoner når disse får innflytelse på politiske beslutningsprosesser i samfunnet. En kritisk befolkning som kan sørge for å holde ulike former for maktgrupperinger og maktfaktorer i tømme, er uunnværlig for at demokrati, frihet og rettigheter vi aldri kan ta for gitt en gang for alle skal opprettholdes.

Disse betraktningene endrer likevel ikke på at det til enhver tid må eksistere rammeverk i form av lover og forskrifter som regulerer og begrenser myndigheters og maktforvalteres makt. Slike skranker mot overdreven maktutøvelse og uforholdsmessig inngripen i menneskers rettigheter og friheter utgjør barrierer både praktisk og psykologisk, og signaliserer at det er og må være grenser for myndigheters og maktstrukturers adgang til å gripe inn i borgernes og enkeltmenneskenes hverdag og liv.

Vi vil i denne høringsuttalelsen ta for oss de nedenfor følgende sektorer som er berørt av Personvernkommisjonen som sentrale i en personvernkontekst, og som det er riktig å fokusere på.

Personvernutfordringer i offentlig sektor og forvaltning

EFN anser at det er nødvendig med et sterkt søkelys på mulige og sannsynlige forutsigbare personvernkonsekvenser når personrelaterte data innsamles, lagres og deles, særlig når dette skjer mellom ulike etater og forvaltningsfunksjoner. I disse prosessene vil det være svært krevende for enkeltindivider å få oversikt over hvilke opplysninger som deles og lagres, og det er enda vanskeligere å vite hvordan de delte dataene eventuelt vil kunne brukes nå eller fremover i tid. Dette er rimeligvis vanskelig å forutse både for det enkelte individet og for saksbehandlere som forvalter opplysningene. Siden deling av personopplysninger mellom etater er uunngåelig og ønskelig, ligger nøkkelen til å opprettholde personvernet i offentlig forvaltning i klare retningslinjer for både hvem som skal ha tilgang til dataene og etter hvilke kriterier og hvor mye data som skal kunne lagres og deles.

Etter vårt skjønn er det sentralt at regelverk og praksis fastslår at det ikke skal lagres og deles mer omfattende persondata enn hva som er bedømt som nødvendig for de formål som må defineres klart. Det må her være en forutsetning at minimering av datamengden til hva som er strengt nødvendig brukes som en rettesnor. En innsamling, lagring og deling av data som går ut over hva som er påkrevet for det bestemte formålet må unngås, slik at offentlige etater bare får tilgang til de opplysningene som trengs for å utføre de funksjoner og tjenester som den aktuelle saken tilsier. Nødvendighet og forholdsmessighet er stikkordene her. Er en deling av bestemte personopplysninger ikke nødvendig for å utføre oppgaven, skal delingen heller ikke skje.

Overskuddsdata, det vil si data som gir informasjoner som går ut over den spesifikke funksjonen dataene er innhentet for å oppfylle, skaper alltid risiko for misbruk og også urettferdig diskriminering og bør prinsipielt ikke lagres eller deles. Dette handler om å verne individer og samfunnsmedlemmer mot misbruk og urettferdighet som kan forekomme i gitte situasjoner, men det handler i høy grad også om det helt fundamentale tillitsforholdet mellom samfunnsborgerne og

forvaltningsorganene. Du skal som medlem av samfunnet kunne ha tillit til at de som forvalter dine persondata, er seg sitt ansvar bevisst og begrenser både innhenting og deling av opplysninger om deg til det minimum som til enhver tid er nødvendig.

I denne sammenhengen er det også sentralt at de individene som får sine personrelaterte data innsamlet, lagret og delt i størst mulig utstrekning får innsyn i og kontroll med hvilke data som samles inn, hva formålet er og hvem som får tilgang til dataene. Dette betyr konkret at EFN støtter det synspunktet at borgerne i størst mulig utstrekning kan få direkte tilgang og fullt innsyn i hva som er registrert om ens person. Rimeligvis kan det i en del kontekster være lettere sagt enn gjort, men å legge bevisste sterke føringer på at dette skal være et overordnet prinsipp bidrar over tid til å gi personvernet en sterkere posisjon i forvaltningen.

EFN mener også at slike overordnede prinsipper bør fastslås av vårt høyeste politiske organ – Stortinget – og at dette må være en åpen og bred prosess som pågår hele tiden i takt med nye personvernutfordringer som måtte melde seg i forhold til særlig teknologiske faktorer som det kontinuerlig må tas stilling til. Det kan ikke alene være opp til de enkelte sektorer å definere hvor grensene for inngrep i privatlivet skal gå, og innsamling og senere deling av persondata er et inngrep.

Det blir da en politisk oppgave å sørge for at dette inngrepet blir minst mulig, og at individene får størst mulig innsyn i hva som er registrert. I forlengelsen av dette, mener vi at det også må foreligge reelle klagemuligheter for borgerne, slik at det er mulig å kreve fjernet opplysninger som kan betegnes som unødvendige eller som overskuddsinformasjon, eller å kreve at feilaktige eller ufullstendige/misvisende opplysninger korrigeres.

En viktig rolle i behandling av persondata innehas av de dataverktøy som brukes for å produsere, lagre og administrere dataene. EFN er av den oppfatning at en forestilling om at store teknologiselskapers og programvareleverandørers løsninger er de mest funksjonelle og tryggeste ikke nødvendigvis er riktig. Det synes i deler av forvaltningen å ha vært en tendens til å anta at de største og mest kjente aktørene også er de som tilbyr de beste teknologiene og verktøyene, noe som etter vår mening er en altfor enkel antakelse som slett ikke alltid holder stikk. Vi vil derfor oppfordre til at det i utvelgelsen av dataverktøy i hvert tilfelle undersøkes hvorvidt løsninger, kanskje spesielt på programvaresiden, som er mer lokalbasert kan være både like gode og til og med å foretrekke ut fra videre hensyn til datasikkerhet og brukerkontroll over verktøyene. EFN mener at det bør være en oppgave for hvert enkelt land å stimulere til utvikling av teknologi og verktøy for datahåndtering, og at dette med fordel kan nedfelles i fastsatte kriterier for innkjøp av dataverktøy til offentlig sektor.

Personvernutfordringer i et generelt forbrukerperspektiv

EFN konstaterer at det for et stort antall ulike markedsaktører er potensielt profitabelt, og derfor nærliggende, å samle inn betydelige mengder persondata for så vel markedsføringsformål som kartlegging av forbrukeratferd helt ned på individnivå. Dette kan i mangel av «checks and balances» utarte til en overvåkningsbasert markedsføring, hvor fortjenestemotiverte markedsaktører foretar en utstrakt sporing og overvåkning av eksisterende eller potensielle kunders atferd med henblikk på å markedsføre presist i henhold til målindividenes egenskaper, det være seg alder, kjønn, hvilke venner man kommuniserer med og hvilke sosiale kontakter de i sin tur har, utdannelse, interesseprofil og foretrukne aktiviteter. Slik registrering av atferd, sosial og personlig profil fører til en massiv innsamling av personopplysninger som til sammen danner

presise mønstre for hvem du «er» som individ. Følgen blir at detaljert kunnskap om individer lagres uten at hverken de registrerte og overvåkte individer eller de som innsamler dataene har noen form for reell kontroll med hvem som kan få tak i dataene, langt mindre med hvordan de kan bli brukt i en nær fremtid eller i et lengre tidsperspektiv. Konsekvensene av denne innsamlingen av personopplysninger kan bli meget alvorlige, med skadenes alvorlighetsgrad avhengig av hvem som får tak i dataene og hvordan de brukes.

Det har i denne konteksten tradisjonelt vært mye fokus på fenomener som identitetstyveri, ulovlig tilegnelse av passord og koder i svindels hensikt og direkte lovbrudd. EFN finner imidlertid at en minst like stor bekymring ligger i den sammenblandingen mellom kapitalinteresser og politikk som vi ser i mange land i varierende omfang. Norge er på ingen måte unntatt. Personopplysninger og atferdsprofiler som er innsamlet av private aktører for markedsføringsformål kan føre til ubotelig skade for individer, dersom disse dataene kommer i hendene på maktfullkomne myndigheter enten som en følge av legale inngrep eller at data som er på avveie samles inn som følge av rutinemessige håndgrep. Når informasjon og personopplysninger først foreligger, kan fristelsen bli uimotståelig til å innsamle og lagre dem. Deretter vil det, i følge «loven» om at dersom data er blitt lagret vil de før eller siden også bli brukt, være vanskelig til umulig å ha noen fremtidig sikkerhet mot at lovlydige borgeres persondata blir benyttet til å gjennomføre uforholdsmessige inngrep mot mennesker. Skadene kan bli meget store, og EFN vil som en første frontlinje for å redusere risikoen for ovennevnte scenarium støtte et forbud mot atferdbasert markedsføring ettersom slik markedsføring er uløselig knyttet til registrering og lagring av individers atferd.

For å konkretisere og sirkle inn problemområder, kan først nevnes internettbaserte tjenester som spesielt aktuelle. Instagram, Facebook, YouTube og TikTok er eksempler på en type tjenester som gitt deres eksistens og funksjon som elektroniske sosiale arenaer vil komme til å samle et stort antall brukere. Disse brukerne vil med nødvendighet måtte benytte tjenestene på slik måte at enorme mengder elektroniske spor og mønstre over interesser, aktitiveter, sosiale kontakter, politiske oppfatninger, seksuelle preferanser og kontakter, livssyn og trosrelaterte oppfatninger, foreningstilknytning og i varierende grad også hva man bruker penger på blir registrert og potensielt lagret.

Hva mer er, de fleste av de funksjonene som de etterhvert meget funksjonsrike nevnte sosiale nettbaserte medier tilbyr gjør det helt umulig å unngå at personopplysninger genereres når man benytter seg av disse digitale og nettbaserte flatene.

For mindreårige gjelder at de er spesielt sårbare for manipulerende påvirkning i markedsføringshensikt. EFN går derfor inn for at det etableres legale skranker mot suggerende former for markedsføring rettet mot mindreårige, og støtter forslag om at det nedsettes et lovutvalg som tar for seg disse problemstillingene.

Nok en problemstilling for den vanlige forbruker er hva som er kjent som biometrisk identifisering. Begrepet dekker bruken av kunstig intelligens («Artificial Intelligence» eller kunstig intelligens (KI)) på norsk, som omfatter bruken av kunstig intelligens som typisk er kombinert med maskinlæring hvor sistnevnte gjennomfører «læring» ved at datasystemene akkumulerer data som samles i mønstre som benyttes i prediktiv analyse. Følgen blir et særdeles alvorlig inngrep i personvernet dersom det tillates at biometriske data om personer, som kroppsform, ansiktsform, gangmønster, stemme samles inn i det offentlige rom. Det er fra flere hold tatt til orde for et generelt forbud mot biometrisk identifisering i det offentlige rom, noe også EFN ser grunn til å gå inn for.

Elektronisk Forpost Norge

Enda en viktig om enn ofte neglisjert problemstilling i en forbrukerkontekst er nettbasert programvare, som er kjent under begrepet «Cloud Computing.»

Historisk har dataprogramvare vært noe lisensinnehaveren («kjøperen») har kunnet disponere over i ubegrenset tid, og dermed installere på så mange datamaskiner som lisensen har gitt adgang til. Det har da ikke vært noen begrensninger på hvor ofte eller når lisensinnehaver har kunnet installere på kompatibel maskinvare. Dette har selvfølgelig ikke innebåret at kjøper/lisensinnehaver har hatt eiendomsretten til programvaren. Man kjøpte imidlertid en lisens, som var evigvarende og ga adgang til i prinsippet uinnskrenket bruk. På 1990-tallet forsøkte en amerikansk programvareaktør å innføre kopisperrer på sine programvareprodukter, noe som førte til store rettssaker som programvareselskapet tapte fordi det ble fastslått at den som kjøpte en lisens på et dataprogram måtte ha en rett til å ta sikkerhetskopi for å sikre at investeringen var varig slik at programvaren kunne de-installeres og re-installeres etter behov. Rundt år 2000 kom så Microsoft med Product Activation, som innebærer at programvaren ikke kan installeres og brukes uten en lisenskontroll med registrering hos programvareselskapets aktiveringstjenester. Snart etter innførte Adobe det samme, i likhet med et knippe andre programvareselskaper som hadde etablert en slik markedsandel at de nærmest hadde oppnådd monopol. En del databrukere responderte med kontant å si nei takk og gå over til Linux og open source-basert programvare, mens flertallet var fornøyd hvis de trykket på knappen og programmet startet uten å reflektere noe særlig over premissene for sin bruk av datamaskinen. Med majoritetens aksept var ikke veien lang til konseptet Software-as-a-Service (SaaS) og nettbasert programvare hvor lisensen og bruken er gjort avhengig av oppkoplinger og abonnement. Å gjøre funksjoner og verktøy om til tjenester er utvilsomt profitabelt for noen aktører, men skaper en alvorlig sårbarhet og medfører en alvorlig svekket råderett over verktøyene vi trenger i dagliglivet.

Programvare som en tjeneste i stedet for noe man disponerer fritt og i ubegrenset tid lokalt på egen maskin innebærer ikke bare opphør av brukerkontroll og fravær av sikkerhet for å beholde sine verktøy, men også øket risiko for at registrerte opplysninger om bruk kommer på avveie – noe som særlig er aktuelt hvis også lagringen av ens produsert data foregår hos en ekstern tjenesteleverandør i stedet for på egne systemer. EFN fraråder på generelt grunnlag bruk av Cloud Computing med mindre det er snakk om interne nettverk i form av en lokalt kontrollert «Own Cloud», og oppfordrer til bevisst valg og bruk av brukerkontrollert programvare som kjøres fra den enkelte enhet både for privatpersoner, institusjoner og bedrifter.

Personvern innenfor justissektoren

Personvernproblematikk innenfor denne sektoren er hovedsakelig knyttet til hvilke grep vi velger å benytte oss av i bekjempelse av kriminalitet. EFN vil påpeke at i et scenarium hvor den overordnede prioriteringen innen justisområdet er å søke å drive gjennom hva som oppfattes å være de mest virksomme kriminalitetsbekjempelsestiltak, vil følgen bli at sentrale rettssikkerhetsprinsipper og skranker mot myndigheters maktovergrep bli stadig mer utfordret. Følgen av en slik situasjon blir med stor sikkerhet at personvern og rettssikkerhet blir presset og i verste fall nedprioritert bevisst eller ubevisst. Ulike former for datalagrings- og overvåkningsproblematikk har vært og er fortsatt i denne konteksten høyaktuelle.

I spørsmål om overvåkning og kontroll vil vi i EFN på det sterkeste fremheve at overvåkningen inntrer i det øyeblikk data i form av vanlige persondata, lokasjonsdata, kommunikasjonsdata eller biometriske data registreres og lagres. Det er altså på ingen måte slik at overvåkningen først etableres hvis og når dataene brukes. Forståelsen for denne realiteten er og må være helt avgjørende når overvåkningsproblematikk og barrièrer mot overvåkning drøftes.

Elektronisk Forpost Norge

Ettersom justisområdet er området for rettslige inngrep mot individer, inngrep som i følge sin natur er de potensielt mest inngripende handlinger som et lands myndigheter kan utføre overfor sine borgere, er det av overordnet viktighet at menneskerettigheter og hevdvunne rettsstatsprinsipper som den grunnleggende uskyldspresumpsjonen og legalitetsprinsippet om at alle inngrep må være hjemlet i lov konsekvent opprettholdes.

Videre er det sentralt for borgernes rettssikkerhet at domstolskontrollen over politiets virkemiddelbruk og inngrep mot individer opprettholdes og forsterkes i samsvar med nye teknologiske overvåknings- og kontrollmuligheter som dersom de benyttes i altfor stor grad skaper en betydelig risiko for en gradvis og umerkelig men ubønnhørlig forvitring av rettsstaten og befolkningens rettssikkerhet. Her vil vi også fremheve biometrisk identifisering som en betydelig risiko. I et scenarium hvor myndigheter og politi kan kartlegge og komme til kunnskap om hvem som har vært på et bestemt sted på et bestemt tidspunkt også når det gjelder individer som ikke er under noen form for mistanke, vil det med overveiende sannsynlighet oppstå en stadig økende nedkjølingseffekt («Chilling Effect») med gradvis uthuling av retten til fri forsamling og frie ytringer til følge.

Personvern i barnehage og skole

EFN mener at digitaliseringen av barnehagers og skolers aktiviteter har skapt store utfordringer for mindreåriges personvern. Barn mangler reelle muligheter til å gi samtykke eller avslå samtykke når teknologiske løsninger ukritisk innføres i slike sammenhenger. For barn er hva som er aktuelt markedsføringstiltak rettet mot mindreårige og lett påvirkelige individer, og disse har behov for særskilt beskyttelse mot de virkninger markedsføringskampanjer rettet mot mindreårige kan ha. EFN mener at det kan være aktuelt å utvikle innenlandske teknologiske løsninger, slik at vi kan unngå kommersielle markedskrefters påvirkning av barn og unge i barnehage og skole.

Personvernutfordringer i forhold til kunstig intelligens

I forhold til kunstig intelligens kan vi observere at KI i likhet med svært mange teknologier ofte benyttes ukritisk, det vil si at den appliseres på områder eller i omfang hvor appliseringen er uhensiktsmessig eller uforholdsmessig.

Kunstig intelligens er ubetinget funksjonell og ønskelig når den appliseres i produksjonsprosesser og rutineoppgaver hvor menneskelige vurderinger, avveininger og valg basert på disse ikke er aktuelle. Hvis KI derimot benyttes i oppgaver hvor menneskets egenvurderinger, avveininger og beslutninger fortrenges av teknologien kan dette i svært mange situasjoner føre til uheldige eller direkte skadelige virkninger som kanskje først erkjennes etter lengre tid. Hvis kunstig intelligens erstatter og fortrenger menneskets evner og ferdigheter skaper det sårbarhet, og det er da viktig å huske på at hva som gir høyest målt «effektivitet» langt oftere enn vi tror er noe helt annet enn hva som er de mest robuste løsningene i et større perspektiv og på lang sikt.

Kunstig intelligens brukt i beslutningssystemer og saksbehandlingskontekster er et annet eksempel på potensielle fallgruber. Det er en utbredt oppfatning at kunstig intelligens og maskinlæringsmodeller gir bedre og riktigere beslutningsprosesser og avgjørelser enn hva menneskets hjerne kan klare. Denne oppfatningen er innenfor en del områder misforstått og til dels sterkt villedende. Menneskets mulighet til å gjøre feil er nært forbundet med evnen til å bruke skjønn og vurdering, fordi det ene uløselig følger det andre. Følgelig må det anses som tvilsomt om det foreligger grunnlag for å si at maskiner er «bedre» enn mennesker når vi som sagt beveger

oss utenfor de mer utpregede rutineoppgaver. Det betyr at automatiserte beslutningsprosesser og avgjørelser basert på kunstig intelligens kan føre til urimeligheter, direkte overgrep og uoverskuelige følger når den menneskelige vurdering elimineres.

Det ofte underliggende premisset om at en datamaskin ikke kan gjøre feil, og at menneskers tilbøyelighet til også å gjøre feil innebærer at KI bør erstatte menneskelige beslutninger i alle sammenhenger hvor statistisk sannsynlige utfall kan danne mønstre som kan gjenkjennes av maskinlæringsmodeller, er atskillig mindre pålitelig enn vi kanskje har vent oss til å tenke.

For et individ som får sin sak avgjort av algoritmer i et datasystem, vil det trolig kunne være ytterst problematisk å få gjennomslag for et synspunkt om at avgjørelsen var urimelig eller feilaktig. Det har vært antydet at det her gjelder å gjøre beslutningsprosessen i systemet «gjennomsiktig», men problemet med det resonnementet er imidlertid at gjennomsiktighet og etterprøvbarhet synes lite realistisk å oppnå når beslutningen er basert på en automatisert mønsterbasert «oppskrift» hvor det menneskelige skjønn og menneskets vurdering er sjaltet ut og eliminert. Konklusjonen må bli at løsningen her, som i en rekke andre kontekster, ligger i å bevisst etablere grenser for teknologiens anvendelsesområde. En slik avgrensning av teknologier er noe som erfaringsmessig faller vanskelig for mennesker, men som er nødvendig å foreta hvis vi skal opprettholde et i videste forstand menneskelig samfunn.

Internasjonale faktorer – for Europa spesielt vedrørende EU

Ofte har det blitt antydet at hva vi ikke klarer å gjennomføre i de enkelte land, må kunne iverksettes på overnasjonalt nivå og at dette er å foretrekke fremfor at hver enkelt befolknings folkevalgte parlamenter har den ultimate myndighet. Dette er i likhet med mange utsagn korrekt i forhold til et gitt sett med premisser, samtidig som det kan være helt feilaktig i forhold til andre premisser. På endel områder har EU-lovgivning uten tvil hatt en nyttig og ønskelig funksjon, og EUs personvernforordning (GDPR-General Data Protection Regulation) er et forsøk på å ivareta personvernet på et européisk nivå. Det er når dette skrives også på trappene en generell EU-forordning om digitale tjenester, og det er også under forberedelse en AI Act – en lov som regulerer bruken av kunstig intelligens.

Situasjonen er den at beslutninger truffet på overnasjonalt nivå i EU-organene, og som munner ut i forordninger og direktiver i EU-rådet og EU-parlamentet, blir legalt bindende for samtlige land og befolkninger som er tilknyttet EU/EØS. Dette setter i praksis de enkelte folkenes egne folkevalgte parlamenter ut av spill, og reiser et demokratisk problem fordi gjennomføring eller avvisning av beslutninger fjernes fra de enkelte folkenes egen autoritet. En forventning om at EU skal være en i hovedsak positiv kraft på personvernets eller andre områder, bygger derfor på et håp om at de beslutningene som treffes sentralt i EU-organene til alle tider er de beste for de tilsluttede landene. En slik forventning om EUs autoritet er ikke nødvendigvis realistisk, og det kan derfor antydes at vernet om menneskerettigheter, personvern, utforming av lover og regelverk på ulike områder samt demokratisk medbestemmelse i videste forstand, med fordel kan ligge hos de enkelte lands folkevalgte parlamenter i en langt større utstrekning enn EU-systemet i 2023 synes å legge opp til.