Rammeverk for behandling av personopplysninger for VID

Innholdsfortegnelse

1.Innledning

1.1 Formål

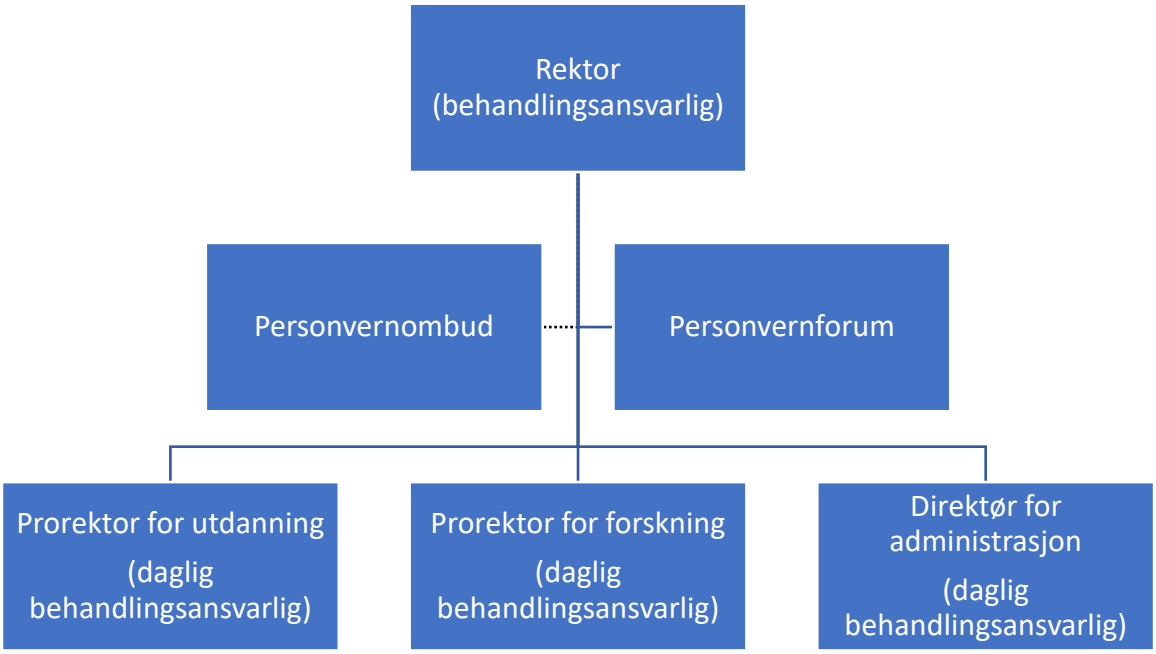
VID vitenskapelige høgskoles (VIDs) rammeverk for behandling av personopplysninger skal sikre at personvernet til studenter, medarbeidere, gjester eller forskningsdeltakere ivaretas. Rammeverket etablerer regler og prinsipper for hvordan VID skal etterleve kravene i EUs personvernforordning (GDPR), som innlemmes i norsk rett gjennom EØS-avtalen og personopplysningsloven. Rammeverket skal sikre at VID behandler personopplysninger på en lovlig og sikker måte, i samsvar med grunnleggende personvernhensyn. Rammeverket skal brukes sammen med hjelpedokumenter som etablerer konkrete rutiner.

1.2 Anvendelsesområde og målgruppe

Rammeverket gjelder for ansatte, studenter, gjester og alle som har tilgang til og/eller bearbeider og forvalter personopplysninger gjennom VIDs infrastruktur.

2.Roller og ansvar

2.1 Organisasjonskart



2.2 Personvernorganisasjon

Rektor

Rektor er behandlingsansvarlig ved VID og har det overordnede ansvaret for behandling av personopplysninger. Rektor bestemmer formålet med behandling av personopplysninger og hvilke verktøy som skal benyttes i behandlingen, altså hvordan personopplysninger skal behandles. Rektor har det overordnede ansvaret for å sikre og dokumentere at all behandling av personopplysninger i VID, eller på vegne av VID, er i henhold til personvernregelverket og kravene som beskrevet nærmere i rammeverket. Rektor skal utpeke daglige behandlingsansvarlige.

Daglig ansvar

Prorektor for utdanning, prorektor for forskning og direktør for administrasjon har det daglige ansvaret for behandling av personopplysninger i VID innen sine respektive ansvarsområder, og for at personvernregelverket og kravene som beskrevet nærmere i rammeverket etterleves.

Systemeiere

Prorektor for utdanning, prorektor for forskning og direktør for administrasjon er eiere av systemer og tjenester innenfor sine respektive ansvarsområder. Systemeierne er ansvarlig for å utvikle, forvalte og drifte informasjonssystemer, og for at personvernregelverket og kravene som følger av rammeverket etterleves.

Systemeieres ansvarsområder er:

- Påse at formålet med og verktøy som benyttes i behandlingen er innmeld på forskriftsmessig vis
- Bestemme formålet med behandlingen av personopplysninger og hvilke verktøy som skal brukes
- Foreta risikovurdering av sikkerheten til personopplysningene
- Inngå avtale med databehandler som drifter systemet eller tjenesten på vegne av VID
- Melde systemet eller tjenesten til personvernombudet ved VID
- Dokumentere at behandling av personopplysninger gjøres i henhold til de til enhver tid gjeldene personvernregler.
- Alle systemer skal føres inn i *Protokoll over behandlingsaktiviteter*, som skal oppdateres jevnlig.

Personvernombud

VID benytter et personvernombud (PVO) i 40 % stilling, som er ansatt ved Stiftelsen det norske diakonhjem. Personvernombud er en uavhengig andrelinjefunksjon som skal oppnevnes av Datatilsynet. Hensikten er å styrke VIDs evne til å etterleve regelverk for behandling av personopplysninger. Personvernombudet rapporterer sine funn og anbefalinger til virksomhetens øverste ledelse, men er ikke underlagt virksomhetens øverste ledelses instruksjonsmyndighet. Personvernombudets rolle og oppgaver følger av EUs personvernforordning artiklene 37, 38 og 39. Personvernombudet har taushetsplikt.

Personvernombudets ansvarsområder er:

- Gi råd til virksomheten i spørsmål som gjelder behandling og sikring av personopplysninger, dette involvere godkjenne DPIA, bidra til ROS juridisk avtaler i personvern området, interne rutiner og gå gjennom avtaler, og gi råd til data behandlinger i flere prosjekter.,
- Kontaktperson for de registrerte som VID behandler personopplysninger om (studenter, medarbeidere, gjester, forskningsdeltakere m.m.).
- Føre kontroll med at behandling av personopplysninger skjer på en lovlig måte, blir varslet og involverte personvernforum og internkontroll arbeidet.
- Samarbeide med Datatilsynet
- Kontaktpunkt for Datatilsynet ved spørsmål om behandling av personopplysninger, herunder forhåndsdrøftelser nevnt i EUs personvernforordning artikkel 36
- Ved behov rådføre seg med Datatilsynet om eventuelle andre spørsmål

Personvernforum

Personvernforum er en ressursgruppe for personvern og informasjonssikkerhet i VID. Gruppen består av personer med særlig kompetanse og ansvar for personvern- og informasjonssikkerhet, samt representanter fra ulike virksomhetsområder.

Ressursgruppens ansvarsoppgaver er:

- Sikre sammenheng i interne reglement, rutiner og retningslinjer
- Avklare spørsmål av overordnet juridisk og praktisk art, herunder utforme og sikre etterlevelse av tilgangskontroll i systemer, lokasjoner, arbeidsplasser og andre steder av relevans for informasjonssikkerhet
- Drøfte og belyse relevante utfordringer og spørsmål fra virksomheten
- Sikre rådgivning og kontroll innenfor relevant fagansvar

- Bistå med opplæring, kompetanse og kunnskap knyttet til personvern og personopplysningssikkerhet
- Bistå med arbeidet for å sikre kontroll og risikovurdering knyttet til systemer, gratis og lisensierte, som benyttes av enhver ansatt i virksomheten. Dette gjelder også mer løselig tilknyttede ansatte som har spesifikke oppgaver i en kortere periode
- Bistå med kontinuerlig oppdatering av *Protokoll over behandlingsaktiviteter* etter EUs personvernforordning artikkel 30, som også kan benyttes for komplett oversikt over systemeierskap for IKT-sikkerhetsarbeidet

Sikkerhetsansvarlig

Seksjonsleder for IT er sikkerhetsansvarlig. Arbeid med informasjonssikkerhet faller i mange tilfeller sammen med arbeidet med personopplysningssikkerhet, og det er derfor hensiktsmessig å legge ansvaret samlet. Den sikkerhetsansvarlige rapporterer til rektor, og skal holde rektor informert om alle spørsmål som har betydning for personvern og informasjonssikkerhet ved VID.

Sikkerhetsansvarliges ansvarsområder er:

- VIDs totale sikkerhetspolicy
- Policy for bruk av skytjenester
- Etablering, oppfølgning og vedlikehold av *Styringssystem for informasjonssikkerhet*
- Etablering, oppfølgning og vedlikehold av *Protokoll over behandlingsaktiviteter*
- Sikkerhetsinfrastruktur og programvare
- Etablering av tilgangssystemer
- Opplæring og holdningsskapende arbeid
- Den tekniske delen av ROS-analyser

IT-ansvarlig

IT-ansvarliges ansvarsområder er:

- Hele IT-porteføljen
- Oversikt og oppfølgning av leverandørkontakter
- Oversikt over databehandleravtaler (ofte vedlegg til leverandørkontakter)
- Iverksette god nok støtte for sikkerhet i infrastrukturen og VIDs rutiner

Personvernkontakt

Personvernkontakten er en faglig personvernressurs i VID. Personvernkontaktens ansvarsområder er:

- Gi råd til virksomheten i spørsmål som gjelder behandling og sikring av personopplysninger
- Kontaktpunkt for løpende avklaringer og veiledning
- Involveres i å vedlikeholde VIDs rammeverk for behandling av personopplysninger
- Involveres i utarbeidelse av ROS og DPIA
- Involveres i å etablere avtaler
- Innkalle til møter og lede personvernforum, som er en ressursgruppe for personvern og informasjonssikkerhet i VID (se nedenfor)

Den enkelte medarbeider

Den enkelte medarbeider skal være kjent med og følge rammeverket for behandling av personopplysninger. Plikten skal gjøres kjent for den enkelte medarbeider av nærmeste leder.

Alle medarbeidere skal være informert om taushetsplikten som gjelder for hver enkelt og skal underskrive egen taushetserklæring.

Den enkelte medarbeider har plikt til å melde avvik til den sikkerhetsansvarlige og personvernombudet ved VID. Dette skjer i henhold til rammeverket for behandling av personopplysninger.

3.Definisjoner og begreper

Personopplysninger (personvernforordningen art. 4 nr. 1) alle opplysninger om en identifisert eller identifiserbar fysisk person («den registrerte»). En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, for eksempel et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.

Særlige kategorier av personopplysninger (personvernforordningen art. 9 nr. 1) er personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Behandling av personopplysninger (personvernforordningen art. 4 nr. 2) er enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, for eksempel innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

Registrerte den fysiske personen (for eksempel studenter, medarbeidere, gjester, deltakere i forskningsprosjekter eller annen fysisk person) som en personopplysning knytter seg til, enten direkte eller indirekte.

Protokoll over behandlingsaktiviteter (personvernforordningen art. 30) den behandlingsansvarlige skal føre oversikt over alle behandlingsaktiviteter.

Behandlingsansvarlig (personvernforordningen art. 4 nr. 7) en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke verktøy som skal benyttes.

Databehandler (personvernforordningen art. 4 nr. 8) en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert organ som behandler personopplysninger på vegne av den behandlingsansvarlig.

Felles behandlingsansvarlige (personvernforordningen art. 26 nr. 1) dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og verktøyet for behandlingen, skal de være felles behandlingsansvarlige.

4.Personvernprinsippene og praktiske retningslinjer

4.1 Prinsippet om lovlig, rettferdig og gjennomsiktig behandling

Den behandlingsansvarlige skal behandle personopplysninger på en lovlig, rettferdig og gjennomsiktig måte.

All behandling av personopplysninger skal ha et behandlingsgrunnlag for å være lovlig. De alternative behandlingsgrunnlagene følger av personvernforordningen artikkel 6. Dersom særlige kategorier av personopplysninger skal behandles, må tilleggsvilkårene i artikkel 9 være oppfylt.

Før personopplysninger kan behandles, skal det vurderes om det foreligger et behandlingsgrunnlag. Dersom det finnes flere behandlingsgrunnlag, må VID bestemmes seg for ett grunnlag som gjelder for den aktuelle behandlingen. Behandlingsgrunnlaget skal dokumenteres (i protokoll).

Nedenfor følger en gjennomgang av de alternative behandlingsgrunnlagene.

4.1.1 Personvernforordningen art. 6, 1 (a) og art. 9, 2 (a) – samtykke

Samtykke fra den registrerte innebærer at den registrerte godkjenner at VID kan behandle personopplysninger om dem. Samtykke skal være informert, frivillig, spesifikt, utvetydig, gitt gjennom en aktiv handling, dokumenterbart og mulig å trekke tilbake like lett som det ble gitt. Forhåndsutfylte bokser eller passivt samtykke er ikke lov. Samtykke skal alltid være skriftlig dersom særlige kategorier av personopplysninger skal inngå i behandlingen.

Behandling som er basert på avgitt samtykke skal avsluttes dersom samtykket trekkes tilbake eller opphører, med mindre det finnes andre behandlingsgrunnlag som kan hjemle en fortsatt behandling. Behandlingen kan for eksempel avsluttes automatisert ved fjerning av tilganger eller sletting av opplysninger. Det kan også gjøres manuelt, men da skal det utarbeides en rutinebeskrivelse. I tilfeller hvor det ikke finnes andre behandlingsgrunnlag for fortsatt oppbevaring av opplysningene enn samtykke, skal opplysningene slettes dersom samtykket trekkes tilbake.

Dersom det ikke er definert en tidsbegrensning for hvor lenge et samtykke er gyldig, vil samtykkets varighet avhenge av konteksten, omfanget av det opprinnelige samtykket og forventningene til den registrerte. Hvis formålet eller behandlingen endres eller utvikler seg betydelig, er det opprinnelige samtykket ikke lenger gyldig. Dersom dette er tilfellet, må det hentes inn et nytt samtykke.

Sjekkliste for utarbeidelse og forvaltning av samtykker

- Sørg for at behandling av personopplysninger bare er basert på samtykke i tilfeller hvor dette er det mest hensiktsmessige behandlingsgrunnlaget, fordi forvaltning av samtykke er ressurskrevende.
- Sørg for at samtykkeerklæring er klart adskilt fra generelle avtalevilkår og betingelser.
- Dersom det er flere formål, sørg for å gi den registrerte mulighet til å gi separate samtykker til de forskjellige formålene.
- Sørg for at samtykket gis gjennom et aktivt valg.
- Etabler en solid prosess for å ivareta tilbaketrekkingsfunksjonalitet.
- Gi tilstrekkelig informasjon (se rett til informasjon i punkt 5.1).
- Sørg for å ha en oversikt over navn eller andre identifikatorer til personen som samtykker, og tidspunkt for aksept av samtykket.
- Sørg for å ha versjonshåndtering av samtykkeerklæringen.
- Oppdater samtykkene jevnlig og vurder om kontekst eller formål endres.

Hjelpedokumenter: mal for samtykke for forskning, bilde, videobruk osv.

4.1.2 Personvernforordningen art. 6,1 (b) – avtale

Behandlingen er lovlig dersom personopplysningene er nødvendige for å oppfylle en avtale som den registrerte er part i, eller når det foreligger en hensikt om å inngå en avtale. Dersom den registrerte nekter å gi bestemte personopplysninger, vil det bety at avtalen ikke kan oppfylles.

Dersom avtalen inneholder særlige kategorier av personopplysninger, vil avtalen i seg selv ikke være lovlig behandlingsgrunnlag med mindre også et av vilkårene i art. 9 nr. 2 er oppfylt.

4.1.3 Personvernforordningen art 6,1 (c) og art 9, 2 (b) – nødvendig for å oppfylle en rettslig plikt

Behandlingen er lovlig dersom personopplysningene er nødvendig for å oppfylle en rettslig forpliktelse. Dersom VID er pålagt å behandle bestemte personopplysninger, er behandlingen lovlig. Dvs. at behandlingen må fastsettes i en lov som VID er underlagt, for eksempel:

- Universitets- og høyskoleloven

- Lov om arbeidsgivers innrapportering av ansettelses- og inntektsforhold som pålegger VID som arbeidsgiver en rekke rapporteringsplikter
- Lov om skatteforvaltning

4.1.4 Personvernforordningen art. 6,1 (d) og art. 9, 2 (c) – nødvendig for å beskytte vitale interesser

Behandlingen av personopplysninger er lovlig dersom personopplysningene er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser. Dette behandlingsgrunnlaget har et snevert virkeområde. Det må være snakk om behandling av personopplysninger i forbindelse med liv og død, eller fare for helsen. Behandlingsgrunnlaget kan ikke brukes for å legitimere masseinnhenting av personopplysninger.

4.1.5 Personvernforordningen art. 6,1 (e) og art. 9, 2 (e) utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet

Behandlingen av personopplysninger er lovlig dersom personopplysningene er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt. Behandlingsgrunnlaget kan være relevant der private virksomheter er tillagt offentlig myndighet eller oppgaver i allmennhetens interesse. Behandlingen må også ha hjemmel i lov eller forskrift, dvs. at behandlingsgrunnlaget må fastsettes i en lov som VID er underlagt, for eksempel universitets- og høyskoleloven.

4.1.5 Personvernforordningen art. 6,1 (f) behandlingen er nødvendig for å ivareta legitime interesser

En virksomhet kan behandle personopplysninger dersom det er nødvendig for å ivareta legitime interesser som veier tyngre enn hensynet til den enkeltes personvern. Den legitime interessen må være lovlig, klart definert på forhånd, reell og saklig. Videre må behandlingen av personopplysninger være nødvendig for å ivareta denne legitime interessen. VID må foreta en interesseavveiing av VIDs behov for å behandle personopplysningene mot den enkeltes personvern.

For eksempel

- direkte markedsføring (med kundeforhold) og forebygging av svindel
- intern administrasjonsprosess

Dersom formålet kan oppnås på en annen måte som bedre ivaretar personvernet, plikter VID å velge den behandlingen som er minst inngripende for den registrerte.

4.1.6 Personvernforordningen art. 9, 2 – (i) allmenne folkehelsehensyn og (j) arkivformål i allmennhetens interesse, formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål

VID må kunne vise til et supplerende rettsgrunnlag i lovgivning for behandlingen. Det supplerende rettsgrunnlaget vil for eksempel være personopplysningsloven §§ 8 og 9 og helseforskningsloven.

4.2 Prinsippet om formålsbegrensning (personvernforordningen art. 5 b)

VID kan ikke behandle personopplysninger uten et formål. Personopplysninger skal bare brukes til spesifikke, uttrykkelige, angitte og berettigede formål. Alle formål som er tilknyttet høyskolens tjenester, arbeid og IT-løsninger, må være klart beskrevet før behandling kan finne sted. Personopplysninger kan ikke behandles videre på en måte som er uforenelig med disse formålene.

Dersom det er ønskelig å gjenbruke personopplysninger til nye behandlingsformål, skal daglig behandlingsansvarlig gjennomføre vurdering knyttet til gjenbruk. Vurdering skal være skriftlig og inneholde følgende informasjon:

- I hvilken sammenheng er opplysningene samlet inn?
- Er nytt formål forenelig med tidligere formål?
- Skal det involvere særlige kategorier av personopplysninger?

- Mulige konsekvenser og risiko?
- Skal kryptering eller pseudoanonymisering brukes?

Dersom nytt formål ikke er forenelig med det opprinnelige formålet, kan behandlingen til nytt formål bare gjennomføres dersom det foreligger et lovlig behandlingsgrunnlag, for eksempel samtykke fra den registrerte, eller at ny behandling har grunnlag i en lovbestemmelse. Alternativt må de aktuelle opplysningene innhentes på nytt med korrekt angivelse av det nye formålet.

Prinsippet om formålsbegrensning dokumenteres ved protokoll over behandlingsaktiviteter (personvernforordningen art. 30).

4.3 Prinsippet om dataminimering (personvernforordningen art. 5 c)

Behandling av personopplysninger skal begrenses til det som er nødvendig for det lovlige formålet.

Dataminimeringsprinsippet må sees i sammenheng med formålsbegrensingsprinsippet, slik at det bare samles inn personopplysninger (kategori, mengde og omfang m.m.) til det som er strengt nødvendig for å sikre at det bestemte formålet med behandlingen kan gjennomføres. Det betyr at behandling av personopplysninger (innsamling, utlevering, overføring, lagring osv.) bare behandles dersom formålet med behandlingen ikke kan gjennomføres uten slike personopplysninger/behandling.

4.4 Prinsippet om riktighet (personvernforordning art. 5 d)

Personopplysninger som behandles skal være korrekte. Uriktige personopplysninger skal uten opphold oppdateres, dvs. korrigeres eller slettes (art. 16).

Daglig behandlingsansvarlig skal sikre at det vurderes konkret hvorvidt uriktige personopplysninger skal slettes eller korrigeres.

VID skal sikre og dokumentere at personopplysninger som behandles, er korrekte, fullstendige og relevante. Ved oppdatering skal nye opplysninger legges inn med ny datering. Sletting av foreldede opplysninger skal vurderes. Ved retting skal informasjon endres til riktig opplysning uten å slette historikk om registeret.

4.5 Prinsippet om lagringsbegrensninger (personvernforordningen art. 17, punkt 5.6)

Personopplysninger skal slettes når de ikke lenger er nødvendige for formålet de ble hentet inn for.

Opplysninger som ikke lenger er nødvendige og relevante, for å oppfylle formålet med behandlingen skal slettes. Det skal utarbeides og tas i bruk instrukser og rutiner for sletting av personopplysninger i alle relevante arkiver, system, systemløsninger, prosesser og tjenester hos VID.

Ved sletting menes fysisk fjerning av personopplysninger. Anonymisering vil øke datasikkerheten og redusere faren for personvernbrudd. I manuelle arkiv vil dette innebære makulering og lignende handlinger som effektivt fjerner opplysningene. I elektroniske arkiver og elektronisk behandling av data vil sletting som oftest bestå i overskriving av de aktuelle dataene, i en slik grad at de aktuelle dataene ikke lar seg gjenskape. Fysisk destruering av det aktuelle lagringsmediet vil også innebære en sletting av aktuelle data.

Anonymisering, overføring/gjenbruk til annet lovlig formål kan også anses som sletting.

Prinsippet om lagringsbegrensninger gjelder uavhengig av hvor personopplysningene er lagret, det vil si både fysisk og digitalt, strukturert og ustrukturert.

Daglig behandlingsansvarlig skal sikre at:

- Tidsfrister for sletting vurderes og fastsettes konkret for samtlige kategorier av personopplysninger. Konkrete rutiner og frister må dokumenteres og lages, ifølge virksomhetens generelle rutiner om informasjon om lagring og sletting.

- IT-løsninger i størst mulig grad tilrettelegger for automatisert sletting av personopplysninger, og at alle nye IT-løsninger innebygger tidsfrister for sletting. Manuell sletting skal fastsettes og gjennomføres der automatisert sletting er teknisk uhensiktsmessig.
- Tilgang til lagrede personopplysninger er i henhold til kravene til informasjonssikkerhet

Hjelpedokumenter: rutine for lagring og sletting, og rutine for lagring i ustrukturerte lagringsområder, samt retningslinjer for informasjonssikkerhet

4.6 Prinsippet om integritet

Personopplysninger skal behandles slik at opplysningenes integritet, konfidensialitet og tilgjengelighet beskyttes. Det betyr at personopplysningene som behandles skal vernes mot uautorisert eller utilsiktet innsyn, ødeleggelse, tap og endring (personvernforordningen art. 32) slik at både kravene til personopplysningssikkerhet i personvernregelverket og informasjonssikkerhetsregler etterleves.

Daglig behandlingsansvarlig skal dokumentere god risikostyring og internkontroll knyttet til personopplysningssikkerheten. Risikovurderinger, sikkerhetsnivå og sikkerhetstiltak knyttet til personopplysningssikkerheten er nærmere fastsatt i retningslinjene for informasjonssikkerhet.

5.Registrertes rettigheter og behandlingsansvarliges plikt (GDPR-portalen 59–74)

Rettighetene må ses i sammenheng med personvernprinsippene slik disse er beskrevet i kapittel 4, og særlig prinsippet om ansvarlighet som pålegger den behandlingsansvarlige å sikre at de registrerte får oppfylt følgende rettigheter. Daglig behandlingsansvarlig skal sikre at krav blir innført, og at etterlevelse av kravene blir dokumentert, herunder:

- rett til informasjon
- rett til innsyn
- rett til korrigering
- rett til sletting
- rett til begrensning av behandlingen
- rett til dataportabilitet
- rett til innsigelse
- rett til å motsette seg automatiserte avgjørelser og profilering

Den registrerte skal ha informasjon om hvordan den behandlingsansvarlige behandler personopplysninger. Informasjonen skal utformes så enkelt at de registrerte forstår

- hvordan personopplysninger blir behandlet
- hvilke konsekvenser behandlingen kan ha
- hvilke rettigheter han eller hun har og hvordan disse rettighetene kan tas i bruk

Informasjon skal være lett tilgjengelig på et klart og tydelig språk, og skal være tilpasset den aktuelle målgruppen (for eksempel barna).

Når den registrerte utøver sine rettigheter, skal daglig behandlingsansvarlig besvare anmodningen fra den registrerte senest innen en måned (30 dager) etter at henvendelsen er mottatt (personvernforordningen art. 12 nr. 3). Fristen kan forlenges med ytterligere 2 måneder, dersom antall anmodninger eller anmodningenes

kompleksitet gjør det nødvendig. Den registrerte skal da informeres om forlenget av svarfristen og en begrunnelse for forsinkelsen.

Utøvelse av den registrertes rettigheter skal være gratis for den registrerte (personvernforordningen art. 12 nr. 5). Dersom forespørsel om innsyn gjentas ofte, kan et rimelig gebyr belastes den registrerte. Det samme kan være tilfelle dersom anmodningene er åpenbart grunnløse eller overdrevne. Daglig behandlingsansvarlig skal sikre at PVO informeres og ved behov konsulteres dersom daglig behandlingsansvarlig ønsker å ilegge gebyrer eller avslå anmodning.

5.1 Retten til informasjon

Når den behandlingsansvarlige samler inn personopplysninger fra den registrerte direkte eller via andre skal daglig behandlingsansvarlig sikre at følgende informasjon, jf. personvernforordningen art. 13 nr. 1 a–f) gis til den registrerte:

- navn og kontaktinformasjon til den behandlingsansvarlige eller databehandleren
- kontaktinformasjon til PVO
- formålene med behandlingen, og det lovlige behandlingsgrunnlaget. Dersom behandling er basert på berettiget interesse, skal det informeres om hvilke legitime interesser behandlingen bygger på.
- mottakere av personopplysninger eller kategorier av slike mottakere
- informasjon om eventuell overføring av personopplysninger til et tredjeland
- informasjon som sikrer at den registrerte forstår om personopplysningene er tilstrekkelig beskyttet
- hvor lenge personopplysninger vil bli lagret. Dersom det ikke er mulig skal det gis informasjon om kriteriene som brukes for å fastsette når personopplysningene skal slettes
- informasjon om den registrertes rettigheter slik de går frem av rammeverket, inkludert hvordan rettighetene kan benyttes

Dersom personopplysninger samles inn fra andre enn den registrerte selv, skal den registrerte i tillegg til informasjonen angitt over, ha følgende opplysninger (personvernforordningen art. 14 nr. 2):

- hvilke personopplysninger som er samlet inn
- hvor personopplysningene kommer fra, og om det er offentlige tilgjengelige opplysninger

Hjelpedokumenter: personvernerklæring, informasjon fra samtykkeskjema

Dersom den behandlingsansvarlige skal behandle personopplysningene til et annet formål enn det formålet personopplysningene opprinnelig ble samlet inn for (for eksempel skal overføre informasjon til andre, og den registrerte ikke er informert om dette), skal den registrerte ha informasjon om dette før behandlingen starter.

Dersom den registrerte allerede har informasjonen, utgår plikten til å informere på innsamlingstidspunktet (personvernforordningen art. 14 nr. 3).

Når personopplysninger samles inn fra andre enn den registrerte, skal informasjonen gis den registrerte innen følgende lovpålagte tidsfrist (personvernforordningen art. 14 nr. 3):

- Senest innen en måned etter at personopplysningene er hentet inn.
- Når formålet med innsamlingen er å kommunisere med den registeret senest ved den første kommunikasjonen.
- Når det er planlagt å utlevere personopplysningene til en annen mottaker senest når personopplysningene utleveres første gang.

Den behandlingsansvarlige er *unntatt fra plikten til å gi informasjon* når opplysninger hentes inn fra andre enn den registrerte, i følgende tilfeller (personvernforordningen art. 14 nr. 5):

- når informasjonen som skal gis allerede er kjent for den registrerte
- når det er umulig eller uforholdsmessig vanskelig å informere den registrerte
- når informasjonsplikt vil gjøre det umulig eller i alvorlig grad hindre at formålene med behandlingen kan oppnås
- når innsamling eller utlevering av personopplysningene er uttrykkelig fastsatt ved lov
- når unntaket må holdes fortrolig/konfidensielt som følge av taushetsplikt

Hjelpedokumenter: personvernerklæring, intervjuguide, samtykkeskjema, brev til de registrerte dersom man samler inn personopplysninger via andre.

5.2 Retten til innsyn i egne personopplysninger

Dersom den behandlingsansvarlige behandler personopplysninger om vedkommende, skal den registrerte på forespørsel få innsyn de aktuelle personopplysningene. Den registrerte har rett på kopi av egne personopplysninger så lenge retten ikke krenker andre personers rettigheter og friheter.

Den registrerte har ikke krav på innsyn i egne personopplysninger når

- personopplysningene er brukt i en vurdering/dokument utarbeidet utelukkende for intern saksforberedelse. Det er bare adgang til å gjøre unntak så langt det er nødvendig å nekte innsyn for å sikre forsvarlige interne avgjørelsesprosesser.
- innsyn vil kunne krenke registrertes eller andre fysiske personers rettigheter og friheter som for eksempel der innsyn vil kunne føre til brudd på taushetsplikten
- opplysningen må hemmeligholdes for å hindre avsløre/forfølge straffbare forhold
- det vil stride mot åpenbare og grunnleggende private og offentlige interesser å gi innsyn for eksempel at personopplysningen har stor konkurransemessig betydning eller utlevering kan skade virksomheten sin stilling i en rettslig tvist

Hjelpedokumenter: rutine for innsyn

5.3 Retten til dataportabilitet (personvernforordningen art. 20)

Dataportabilitet er retten til å nærmere vilkår å få overført noen av sine sentrale personopplysninger til seg selv eller en annen virksomhet som en selv utpeker. Den registrerte skal gis tilgang til egne personopplysninger som vedkommende har gitt til den behandlingsansvarlige. Begrepet «provide» må tolkes vidt og inkluderer også

personopplysninger som ikke er aktivt eller bevisst avgitt. Herunder er både informasjon som er mottatt direkte fra den registrerte, og informasjon som er registrert gjennom den registrertes bruk av en tjeneste som er omfattet. For eksempel: søkehistorikk.

5.3.1 Retten til dataportabilitet gjelder ikke når

- personopplysningene kun finnes på papir eller finnes på skannede dokumenter i elektroniske arkiver
- overføringen krenker andres rettigheter og friheter (fysiske personer)
- personopplysningene er samlet inn fra andre kilder enn den registrerte selv
- personopplysningene er utarbeidet for internt bruk på grunn av personopplysninger som samles inn fra den registrerte for informasjon eller analyse

- personopplysningene er samlet inn for å gjennomføre lovpålagte plikter

Automatiserte dataportabilitetsløsninger bør kunne sørge for at dataoverføring skjer raskt etter at den registrerte har sendt en forespørsel. Overføring skal uansett skje «uten ugrunnet opphold» og senest innen en måned etter forespørsel er sendt.

5.3.2 Gjennomføringsprosess

Den registrerte har mulighet både til å laste ned dataene selv for egen bruk og lagring samt å videreføre de direkte til en annen behandlingsansvarlig, for eksempel ved å kunne laste ned opplysninger fra en hjemmeside.

Identifiseringsprosess og sikkerheten må ivaretas. Opplysningen må skje i et format som støtter gjenbruk. Formater som er underlagt lisensbegrensinger, vil heller ikke anses tilstrekkelig.

Overførselen må skje uten unødvendig forsinkelse og senest innen en måned. I komplekse tilfeller kan fristen utvides i inntil tre måneder. Det forutsetter imidlertid at den registrerte har blitt informert om grunnen til forsinkelsen innen en måned fra den opprinnelige forespørselen.

5.4 Rett til korrigering

Dersom personopplysninger om den registrerte er unøyaktige eller feil, kan dette få store konsekvenser for den registrerte.

Den registrerte har rett til (jf. personvernforordningen art. 18)

- å få uriktige personopplysninger om seg selv korrigert uten ugrunnet opphold, dvs. så snart som mulig, samt motta bekreftelse på at dette er utført
- under hensyn til formålene med behandlingen å få ufullstendige personopplysninger komplettert gjennom å fremlegge supplerende dokumentasjon.

5.5 Rett til sletting

Denne rettigheten må ses sammen med lagringsbegrensningsprinsippet i punkt 4.5.

5.6 Rett til begrenset behandling

Den registrerte har rett til å kreve begrenset behandling av egne personopplysninger. Det innebærer at personopplysningene ikke kan brukes, bare lagres (personvernforordningen art. 18 a–d).

Begrenset behandling kan kreves i følgende tilfeller:

- Dersom den registrerte mener at personopplysningene er unøyaktige, kan behandlingen begrenses i en periode, slik at både den registrerte og den behandlingsansvarlige kan kontrollere om personopplysningene er riktige, og eventuelt foreta korrigering.
- Behandlingen er ulovlig, men den registrerte motsetter seg sletting og krever isteden at bruken begrenses, og at personopplysningen dermed fortsatt lagres.
- Den behandlingsansvarlige trenger ikke lenger opplysningen til formålet med behandlingen, men den registrerte har behov for opplysningene for å fastsette, gjøre gjeldende eller forsvare et rettskrav og ønsker derfor at personopplysningene fortsatt lagres.
- Den registrerte har protestert på behandlingen og avventer tilbakemelding på vurdering av om den behandlingsansvarliges berettigede grunner for behandling går foran den registrertes.

Dersom behandlingen er blitt begrenset, skal personopplysningene lagres og bare behandles dersom (personvernforordningen art. 1 8 nr. 2)

- den registrerte har samtykket til behandlingen.

- når det er nødvendig for å fastsette, gjøre gjeldende eller forsvare et rettskrav.
- man må beskytte en annen fysisk eller juridisk persons rettigheter

Når en begrenset behandling oppheves, skal den registrerte informeres om dette.

5.7 Rett til underretning

Dersom den behandlingsansvarlige har utlevert personopplysninger om den registrerte til bestemte mottakere, skal samtlige mottakere informeres (personvernforordningen art. 19) om enhver korrigering (art. 16), sletting (art. 17 nr. 1) eller begrenset (art. 18) behandling som den behandlingsansvarlige gjennomfører.

Den registrerte har også en rett til å bli underrettet om et brudd på

personopplysningssikkerheten (personvernforordningen art. 34) kapittel 4.6.2. Den behandlingsansvarlige skal uten ugrunnet opphold underrette den registrerte om et brudd på personopplysningssikkerheten dersom det trolig er at nevnte brudd kan medføre en høy risiko for den fysiske personens rettigheter og friheter, slik at vedkommende får muligheten til å ta nødvendige forhåndsregler.

Underretningen skal inneholde

- en klar og tydelig beskrivelse av bruddets art
- kontaktopplysningene til PVO eller annet kontaktpunkt der mer informasjon kan innhentes
- en beskrivelse av de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten
- en beskrivelse av de tiltakene den behandlingsansvarlige har satt i verk eller foreslår å sette i verk for å håndtere bruddet
- relevante tiltak for å redusere eventuelle skadevirkninger som følge av bruddet

Underretning til den registrerte er ikke nødvendig dersom et av følgende vilkår er oppfylt:

- Den behandlingsansvarlige har gjennomført egnede tekniske og organisatoriske sikkerhetstiltak og disse tiltakene er blitt anvendt på personopplysningen som er berørt av bruddet på personopplysningssikkerheten, særlig tiltak som gjør personopplysningene uleselige for enhver person som ikke har autorisert tilgang til dem, for eksempel kryptering.
- Den behandlingsansvarlige har truffet etterfølgende tiltak som sikrer at det er lite trolig at den høye risikoen for de registrertes rettigheter og friheter inntreffer.
- Det vil innebære en uforholdsmessig stor innsats. Dersom dette er tilfellet, skal allmennheten isteden underrettes, eller det skal settes i verk et lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte.

De registrerte bør underrettes så snart det med rimelighet er mulig og i nært samarbeid med tilsynsmyndigheten.

6.Oversikt over behandling av personopplysninger (protokoll)

Daglig behandlingsansvarlig skal sørge for at det blir ført oversikt over behandling av personopplysninger som utføres i vedkommende enhet. Oversikten skal inneholde informasjon som går frem av EUs personvernforordning artikkel 30.

Hjelpedokumenter: mal for å utarbeide protokoll

Meldingsregisteret til Norsk senter for forskningsdata (NSD) gir en oversikt over behandling av personopplysninger i forskningsprosjekter.

7.Vurdering av personvernkonsekvenser (DPIA)

Hvis det er sannsynlig at en type behandling vil medføre høy risiko for enkeltpersoners rettigheter og friheter, skal den behandlingsansvarlige foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personvernet, jf. artikkel 35.

Vurderingsspørsmål om behov for DPIA. Dersom svaret er «ja» på to eller flere av spørsmålene nedenfor, kan det bety at det er behov for DPIA.

7.1 Prosess for utarbeidelse av DPIA

Forhåndsvurdering av om DPIA skal utarbeides (prosjektleder/systemeier)

Gjennomføring (prosjektleder/systemeier) involvering av PVO godkjenning av DPIA (nærmeste leder for systemeier og prosjektleder)

Systemeier/prosjektleder skal sørge for at det blir utført en DPIA der det er krav om dette. Vedkommende skal rådføre seg med personvernombudet. Dette gjelder også om vedkommende er i tvil om det er nødvendig med en DPIA.

7.2 Vurderingsspørsmål

a) Personopplysninger samlet inn via en tredjepart i følge med minst ett annet kriterium.

b) Behandling av biometriske opplysninger for å identifisere enkeltpersoner i følge med minst ett annet kriterium.

c) Behandling av genetiske opplysninger i følge med minst ett annet kriterium.

d) Behandling av personopplysninger med innovativ teknologi i følge med minst ett annet kriterium.

e) Behandling av personopplysninger, uten samtykke, for vitenskapelige eller historiske formål i følge med minst ett annet kriterium.

f) Behandling av lokasjonsdata i følge med minst ett annet kriterium.

g) Behandling av personopplysninger for systematisk monitorering av ansatte.

h) Behandling av personopplysninger for å evaluere læring, mestring og trivsel i skoler eller barnehager.

1) Dette inkluderer alle utdanningsnivåer: barne- og ungdomsskole, videregående skoler og høyere utdanning. (Sårbare registrerte og systematisk monitorering.)

i) Systematisk monitorering, inkludert kameraovervåking, på offentlig tilgjengelige områder i stor skala. (Systematisk monitorering og stor skala.)

j) Kameraovervåking i skoler og barnehager i åpningstider. (Systematisk monitorering og sårbare registrerte.)

k) Behandling av særlige kategorier av personopplysninger eller svært personlige opplysninger i stor skala for algoritmetrening.

l) Behandling av personopplysninger ved å systematisk monitorere effektivitet, ferdigheter, kunnskap, mental helse og utvikling. (Svært personlige opplysninger og systematisk monitorering).

m) Behandling av personopplysninger der formålet er å tilby en tjeneste eller utvikle produkter for kommersiell bruk som involverer å forutsi jobbprestasjoner, økonomi, helse, personlige preferanser eller interesser, pålitelighet, adferd, lokalisering eller bevegelsesmønster. (Særlige kategorier av personopplysninger eller svært personlige opplysninger og evaluering/poengsetting.)

n) Innsamling av personopplysninger i stor skala gjennom «tingenes internett» eller velferdsteknologi. (Stor skala og særlige kategorier av opplysninger eller svært personlige opplysninger.)

Dersom du svaret et ja til spørsmål A–F i tillegg til et ja til spørsmål A–N, eller det er et ja til spørsmål G–N, er det nødvendig å gjennomføre DPIA i samsvar med Datatilsynets krav.

Når er en personvernskonsekvensvurdering (DPIA) ikke nødvendig å gjennomføre:

- når det ikke er sannsynlig at behandlingsaktiviteten vil medføre høy risiko for fysiske personers rettigheter og friheter, jf. art. 35 nr. 1
- Når omfanget, konteksten og formålet med behandlingsaktivitet er svært lik en behandlingsaktivitet som allerede har blitt utført en personvernkonsekvensvurdering brukes, jf. art 35 nr. 1.
- når en behandlingsaktivitet har blitt godkjent av Datatilsynet i henhold til direktiv

  95/46/EF før mai 2018, og de spesifikke forholdene ikke er endret, jf. fortalepunkt 171
- når en behandlingsaktivitet, i tråd med art. 6 nr. 1 bokstav c eller e, er lovregulert der loven regulerer den spesifikke behandlingsaktiviteten, og hvor en DPIA allerede har blitt gjennomført som en del av grunnlaget for lovreguleringen, unntatt hvis lovgiveren har erklært det nødvendig å gjennomføre en DPIA for den aktuelle behandlingsaktiviteten, jf. art. 35 nr. 10

når behandlingen er inkludert på listen over behandlingsaktiviteter som ikke krever personvernkonsekvensvurdering jf. art 35 nr. 5. I slike tilfeller kreves det ikke en personvernkonsekvensvurdering, unntatt hvis databehandlingsaktiviteten faller strengt innenfor rekkevidden av den aktuelle behandlingen som er nevnt i listen og fortsetter å oppfylle alle de relevante kravene i personvernforordningen.

Hjelpedokumenter: mal for å utarbeide DPIA

8.Risikovurderinger

En risikovurdering er et verktøy for å identifisere uønskede hendelser og risikoen for at de skal inntreffe. Virksomheten skal gjennomføre risikovurdering før man:

setter i verk en behandling

- før enheten kjøpe inn nytt utstyr eller tar i bruk et informasjonssystem som innebære behandling av personopplysninger.
- ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel endringer i behandlinger, endringer av informasjonssystem eller endringer i trusselbildet.

Linjeleder skal påse at det blir gjennomført risikovurderinger ved enheten. Linjeleder skal gjøre seg kjent med viktige risikoforhold. På bakgrunn av risikovurderinger skal linjeleder sørge for at det utarbeides handlingsplaner og blir gjennomført tiltak for å minimere risiko.

System eier eller prosjekt ansvarlig skal ta hoved ansvar å gjennomføre risikovurdering.
Informasjonssikkerhets rådgiver og PVO, Personvern Kontakt (forsknings området) skal kontakts for å bidra til risikovurdering hvis nødvendig.

Datatilsynets veiledning

For å kunne vurdere hvilke sikkerhetstiltak som er egnet, må enheten foreta en risikovurdering. Risikovurderingen må foretas ved å ta hensyn både til sannsynligheten for at personopplysningene kommer på avveie, skades, stjeles, endres eller behandles ulovlig, og hvor alvorlige konsekvenser det vil ha dersom dette

skulle skje. I noen tilfeller kan sannsynligheten være lav, men de alvorlige konsekvensene være veldig høye, og da må risikoen fremdeles tas på alvor.

8.1 Prosess

Steg 1: Identifikasjon av uønskede hendelser

Dette kan for eksempel være brudd på konfidensialitet/spredning til uvedkommende, eller at opplysningene går tapt eller blir utilgjengelige.

Steg 2: Angivelse av mulige årsaker til hendelsen

Dette kan for eksempel være svikt i sikkerhetsrutiner, passord på avveie og lignende.

Behandling: enhver bruk av personopplysninger, både innsamling, lagring, systematisering eller formidling

Steg 3: Anslå sannsynligheten for at hendelsen inntreffer

Anslå sannsynligheten for at hendelsen inntreffer med en tallverdi mellom 1 og 5, der 1 representerer minst sannsynlig og 5 representerer mest sannsynlig.

Hvis hendelsen for eksempel kan inntreffe ved de ansattes uaktsomhet, eller om utenforstående har en særlig motivasjon for å få tilgang til opplysningene, er dette forhold som kan medføre at hendelsen vurderes som sannsynlig (4) eller meget sannsynlig (5).

Steg 4: Anslå konsekvensen

Anslå hvor betydelig konsekvensen vil være for vernet av personopplysninger der en mulig hendelse inntreffer, med en tilsvarende skala på 1–5. Her vil det være relevant å se på konsekvensene for den registrerte, men også for enheten. Hvis hendelsen for eksempel kan medføre omdømmetap, erstatningskrav eller andre sanksjoner, er dette forhold som kan medføre at konsekvensen settes til alvorlig (4).

Steg 5: Kalkuler risikoen

I den siste raden skal tallverdien for sannsynligheten multipliseres med tallverdien for konsekvensen, og man har fått et uttrykk for risikoens størrelse. For eksempel 3

(sannsynlighet for hendelse) × 4 (størrelsen på konsekvens) = 12 (risikoens størrelse).

Steg 6: Plasser hendelsene i risikotabellen

De skraverte feltene representer uakseptabelt risikonivå. Enheten må her vurdere hvilke sikkerhetstiltak som skal iverksettes for å redusere risikoen til et akseptabelt nivå.

Hjelpedokumenter:

Mal for risikovurdering

risikovurderings mal for skyløsning (med sjekkliste)

risikovurderings mal for dataoverføring til utenfor EØS (med sjekkliste)

8.2 Sikkerhetstiltak

Enheten må sette i verk egnede sikkerhetstiltak på bakgrunn av risikoanalysen. Videre blir det gitt konkrete eksempler på hvordan slike tiltak kan settes i verk.

Det anbefales at enheten oppretter et eget dokument som beskriver hvilke tiltak som er satt i verk. Tiltak bør vurderes i samarbeid med IT-avdelingen eller IT-leverandør og andre relevante deler av administrasjonen som kan sette i verk tekniske og fysiske tiltak som installasjon av antivirusprogramvare, logging av autorisert og uautorisert bruk, installasjon av adgangskontroll og fysisk sikring.

Handlingen kan for eksempel være at personalmapper oppbevares i et låst skap, og at man bruker reservekopieringsløsninger. Av organisatoriske tiltak vil særlig opplæring og bevisstgjøring av enhetens ansatte rundt sikkerhetsansvar være viktig, for eksempel gjennom en IT-instruks. Andre eksempler er tilgjengeliggjøring av sikkerhetsprosedyrer og -mål for de ansatte gjennom intranett, kurs eller liknende, signering av konfidensialitetsavtaler der dette regnes som nødvendig, klare ansvars- og myndighetsforhold for bruk av systemer, jevnlige sikkerhetsrevisjoner og interne prosedyrer for avvikshåndtering.

Det avgjørende vil være at enheten oppnår et tilstrekkelig sikkerhetsnivå i forhold til foreliggende risiko.

Enheten bør av denne grunn ta i bruk rutiner for regelmessig analyse og vurdering av om igangsatte sikkerhetstiltak er tilstrekkelig effektive til å opprettholde sikkerhetsnivået.

Hjelpedokumenter: sikkerhetsinstruks for bruk av datasystemer

Allerede eksisterende IT-instrukser bør gjennomgås og oppdateres med relevante risikoreduserende tiltak for å imøtekomme forordningens krav til informasjonssikkerhet.

9.Overføring/behandling av personopplysninger—Avtaler

Det er den behandlingsansvarlige som har ansvar for behandlingen av personopplysninger og at de behandles etter det formålet som er bestemt. VID både overfører og mottar personopplysninger fra andre. Dette må reguleres gjennom en avtale. For å sikre at mottaker av personopplysninger behandler opplysningene i tråd med GDPR må vi inngå en avtale om overføringen.

For behandling/overføring av personopplysninger skal det brukes én av følgende tre typer:

1. Databehandleravtale
2. Dataoverføringsavtale
3. Avtale om felles behandlingsansvar

Ved tvil om det i det enkelte tilfellet skal benyttes databehandleravtale eller andre avtaler, skal personvern-kontakt eller PVO på virksomhetsstyring kontaktes før overføring finner sted.

1. Der IT-avdelingen anskaffer programvare/ overføre data skal de signere avtalen.
2. Der fakultet eller institutt, forsknings prosjekt anskaffer programvare/ overføre data er de ansvarlige for å etablere databehandleravtale/dataoverførings avtale/ fellesbehandlings avtale. Det er linjeleder som skal signere avtalen.
3. Personvernkontakt (forskingsområdet) og PVO (andre områder) kan bistå med vurdering av databehandleravtale som ikke følger VIDs mal.
4. Når avtalen er signert skal ansvarlig enhet arkivere i sak mappe.
5. Husk å oppdatere oversikten/protokollen over personopplysningsbehandlinger i p360– (adgangsbegrenset)

9.1 Databehandleravtale

Databehandleravtale er obligatorisk (Jf GDPR art. 28).

Når VID setter ut hele eller deler av behandlingen av personopplysninger til en annen virksomhet, er den eller de som behandler opplysningene på VIDs vegne, å anse som databehandlere. For eksempel: tjeneste leverandør. Databehandleravtalen sikrer at personopplysningene kun brukes til sitt angitte formål, at de brukes på VIDs instrukser og i overenstemmelse med personvernregelverket.

Den behandlingsansvarlige må ha full oversikt over alle sine databehandlere og underleverandører. Daglig behandlingsansvarlig har det utførende ansvaret for at rutinen etterleves.

Databehandleravtalen skal lagres i saks- og arkivsystemet. Det skal etableres egen arkivsak for hver leverandør.

VID har utarbeidet standard databehandleravtale som i utgangspunktet skal brukes. Hvis standardavtalen ikke kan brukes, skal den forelagte avtalen kontrolleres opp mot denne.

Avtalen skal også vurderes av personvern kontakt (forskningsprosjekt) eller PVO før den blir inngått. (Enheten må ha tydelig roller og ansvar beskrivelse om dette.)

Hjelpedokumenter:
Mal for databehandleravtale

Data Processing agreement

9.2 Dataoverførings avtale

Når VID som behandlingsansvarlig overfører personopplysninger til en annen selvstendig behandlingsansvarlig, skal det ikke inngås databehandleravtale. Mottaker av opplysningene håndterer ikke disse på vegne av VID og er selvstendig ansvarlig for å etterleve GDPR, Dette vil være tilfelle i mange av de samarbeids prosjekter VID deltar i.

I slike tilfeller er mottaker ansvarlig for å etterleve GDPR. VID på sin side må være sikker på å ha rettslig grunnlag for slik overføringen.

Mal for dataoverføringsavtale (.docx)
Template Data Transfer Agreement between two Data Controllers (.docx)

9.3 Avtale om felles behandlingsansvar

Dersom VID sammen med andre selvstendig behandlingsansvarlige bestemmer formål med og midler for databehandlingen, foreligger et delt behandlingsansvar.
Avgjørende er hvorvidt de involverte parter i fellesskap har bestemmende innflytelse på mål og midler for den aktuelle behandlingen, eller om det bare er en av partene som bestemmer. Bestemmer de i fellesskap, skal det inngås en avtale som angir partenes ansvar.

Mal for Fellesbehandlings avtale
Template Joint Data Controller Agreement

10.Overføring av personopplysninger til utlandet

10.1 Personopplysninger kan overføres til land i EU og EØS-området

Se datatilsynets nettside.

I alle tilfeller må personopplysningslovens krav til behandling av personopplysninger være oppfylt:

- Vurder om overføringen er i samsvar med grunnkravene i personopplysningsloven.
- Overføring av forskningsdata til utlandet er ikke søknadspliktig/meldepliktig i seg selv, men overføringen må beskrives i en eventuell søknad til REK eller melding til NSD (PVO) knyttet til hovedformålet med behandlingen.
- Det skal inngås databehandleravtale dersom personopplysningene overføres til en databehandler. Hvis opplysningene overføres til en behandlingsansvarlig mellom to databehandlingsansvarlige (se punkt 8) skal grunnlag for hjemmel for overføring vurderes. Dataoverførings avtale skal signeres.
- Vurder om det er nødvendig å utarbeide DPIA, i samsvar med personvernforordningen art. 35. I den forbindelse kan det ha avgjørende betydning om personopplysningene

som planlegges overført, er sensitive eller ikke. Se også retningslinjer om informasjonssikkerhet, under «Hva skal beskyttes?», jf. personvernforordningen art. 45.

10.2 Overføring av forskningsdata til land utenfor EU og EØS-området er som hovedregel ikke tillatt

Overføring av personopplysninger til tredje land (land utenfor EU og EØS-området, land Europakommisjonen ikke har godkjent, og amerikanske virksomheter), kan likevel være tillatt, jf. personvernforordningen § 46.

Det må gjøres en risikovurdering av overføringen for å sikre at informasjonssikkerheten er tilfredsstillende. Risikovurderingen må kunne dokumenteres.

- Overføring til land utenfor EU/EØS kan skje dersom EU-kommisjonen har godkjent at landet har en forsvarlig behandling av personopplysninger (se Rules for the protection of personal data inside and outside the EU).
- 10. juli, 2023, fikk USA en slik *adekvansbeslutning* som innebærer at hvis en amerikansk virksomhet står på lista over godkjente virksomheter (dataprivacyframework.gov), kan det overføres personopplysninger til den som om det var en europeisk virksomhet. For virksomheten som ikke står på listen, må risikovurdering gjennomføres og EU standardkontrakter signeres.
- Overføring utover dette krever at EUs standardkontrakt for overføring til behandlingsansvarlig eller databehandler i tredjeland brukes, eller at overføringen er tillatt etter øvrige punkter i EUs personvernforordning kapittel V. EUs standardkontrakter er tilgjengelige på Datatilsynets nettsider.
- Overføring med hjemmel i EUs personvernforordning artikkel 49 gir unntak for *særlige tilfeller*. Dette gjelder for eksempel dersom den registrerte uttrykkelig har samtykket til aktuell overføring eller overføringen er nødvendig for å oppfylle en avtale som er inngått i den registrertes interesse mellom den behandlingsansvarlige og en annen fysisk eller juridisk person. Eksempel på dette er medlemmer som hører hjemme utenfor EU/EØS, i sakkyndige komiteer.
- Standardkontraktene som er utarbeidet etter det tidligere EU-direktivet i 1995, kan benyttes inntil nye kontrakter er utarbeidet. Tillatelser fra Datatilsynet og EU kommisjonen etter tidligere direktiv eller lov skal fortsette å gjelde frem til de endres, erstattes eller oppheves.

Overføring av forskningsdata til tredje land på dette grunnlaget krever som hovedregel ingen

forhåndsgodkjenning, men overføringen må beskrives i en eventuell søknad til

REK/Datatilsynet eller melding til NSD knyttet til hovedformålet med behandlingen.

Ved overføring av personidentifiserbare helseopplysninger til land utenfor EØS-området må visse krav i helseforskningsloven § 37 være oppfylt.

Hvis forskningsdata er overført til utlandet i forbindelse med forskningen, skal prosjektlederen vite hvordan opplysningene blir håndtert etter at prosjektet er avsluttet. Sluttmeldingen til REK/NSD må inneholde en redegjørelse for hvilke forskningsdata som på avslutningstidspunktet befinner seg i utlandet, og hvem som er databehandler.

Avtale om overføring av personopplysninger til utlandet skal legges frem for IT-seksjonen og vurderes av PVO/informasjonssikkerhetsleder før avtalen blir inngått.

11.Avvikshåndtering ved brudd i behandling av personopplysninger

Formålet med avviksmelding og avvikshåndtering er å håndtere brudd på gjeldende lover, regler samt interne retningslinjer og rutiner. Håndteringen skal gjøre det mulig å gjenopprette tilstanden, fjerne årsaken til avviket, redusere negative konsekvenser for både VID og tredjepersoner, samt bidra til å forhindre fremtidige sikkerhetsbrudd og brudd på personvernet.

Ansatte i VID skal ha kjennskap til rutinen for hvordan avvik ved behandling av personopplysninger skal håndteres. Rutinen skal avdekke og forbedre forhold som ikke tilfredsstiller kravene til personvern.

Et særskilt formål er å sikre effektiv melding til Datatilsynet ved brudd på håndteringen av personopplysninger (innen 72 timer). Det er også et formål å sørge for at berørte registrerte varsles så snart som mulig, slik at de kan ivareta interessene sine.

- Den som oppdager avviket, skal straks varsle avvik til nærmeste leder / daglig behandlingsansvarlig og personvernombudet. Avviket fordeles til riktig *avvikseier (Systemeier/avdelingssjef).*
- Avvikseier følger opp videre med varsling av berørte og tiltak for å lukke avviket.
- Den som oppdager avviket, eller nærmeste leder, rapporterer til daglig behandlingsansvarlig. Hvis avviket er alvorlig eller kritisk for personvernet, skal rektor være avvikseier.
- Personvernombudet melder avviket til Datatilsynet. Personvernombudet skal informeres om avviket så tidlig som mulig. Personvernombudet vurderer om avviket er meldepliktig til Datatilsynet. Datatilsynet skal varsles innen 72 timer.

Hjelpedokumenter: Rutine for avvikshåndtering ved brudd på personopplysningssikkerheten og melding til Datatilsynet.

12.Utlevering av personopplysninger til eksterne

Utlevering av personopplysninger fra VID til andre formål enn det de er samlet inn for, skal godkjennes av daglig behandlingsansvarlig. Daglig behandlingsansvarlig er ansvarlig for at utleveringen blir dokumentert slik at informasjonsplikten ved krav om innsyn fra den registrerte kan ivaretas.

Personer som ikke er underlagt virksomhetens instruksjonsmyndighet, kan ikke få tilgang til organisasjonens systemer med helse- og personopplysninger for selv å hente ut opplysningene.

12.1 Utlevering av personopplysninger om vanlige studenter og ansatte

Informasjon som er innsamlet og lagret for generell personalforvaltning og om ansatte/studenter og andre administrative formål, skal normalt ikke utleveres til utenforstående med mindre de som ber om opplysningene, har rett til innsyn etter lovhjemmel som gi rett til å få opplysningene utlevert.

12.2 Utlevering av helsepersonopplysninger til forskningsprosjekter

Virksomheten kan utlevere personopplysninger til ekstern virksomhet dersom den enkelte pasient har samtykket til deltakelse i det aktuelle forskningsprosjektet og prosjektet er godkjent av REK.

Dersom forskningsprosjektet ikke er samtykkebasert, må REK ha innvilget dispensasjon fra taushetsplikten, eller det må foreligge annen lovhjemmel.

12.3 Håndtering

- Forespørsel om utlevering av personopplysninger/helsepersonopplysninger må alltid rettes skriftlig til virksomheten ved daglig behandlingsansvarlig.
- Prosjektleder må oversende kopi av informasjonsskriv og samtykkeerklæring til virksomheten. (Dersom forskningsprosjektet ikke er samtykkebasert, må kopi av dispensasjon fra taushetsplikten oversendes sammen med en spesifikasjon av hvilke forskningsdata som søkes utlevert.)

- Virksomheten som utleverer opplysninger, må forsikre seg om at opplysningene blir forsvarlig oppbevart etter at de er utlevert.
- Ved utlevering til land utenfor EØS må prosjektleder skriftlig forsikre seg om at den utenlandske databehandlingsansvarlige følger GDPR, og at forskningsdeltakeren har samtykket og er informert om at opplysningene skal utleveres til land utenfor EØS. Avidentifiserte eller pseudonyme data kan utleveres dersom kopling til personidentifikasjoner ikke kan skje så lenge opplysningene befinner seg i utlandet.
- Institusjonen med ansvar for forskningen må sammenstille helse- og personopplysninger før utlevering kan finne sted.
- Ved utlevering til ekstern mottaker: Utlevering av avidentifiserte data (datafil + nøkkelfil) på CD/DVD eller minnepenn: Rekommandert, og i to forsendelser; nøkkelfil og data sendes hver for seg, fortrinnsvis kryptert.
- Utlevering av personopplysninger må ikke skje via åpen e-post eller usikret kommunikasjonsmetode (for eksempel offentlig skyløsning).

  Hjelpedokumenter: Retningslinjer for klassifisering av informasjon

13.Innebygget personvern og personvern som standardinnstilling

Innebygget personvern har som formål å sikre at alle tekniske systemer eller løsninger som virksomheten bruker, blir utviklet på en måte som ivaretar den registrertes personvern. Kravet gjelder der virksomheten utvikler egen programvare, eller bestiller systemer, tjenester og løsninger av andre. Det anbefales at virksomheten inkluderer kravet i eventuelle avtaler med egne leverandører og konsulenter.

For tilfeller der virksomheten skulle være involvert i egen programutvikling, har Datatilsynet utarbeidet en egen veileder for dette. Personvern som standardinnstilling innebærer at virksomheten skal velge de mest personvernvennlige innstilligene som standardinnstilling i gjeldende i IT-løsninger. Personvernet skal tas hensyn til i alle utviklingsfasene av et system:

- Vær i forkant, forebygg fremfor å reparere.
- Gjør personvern til standard innstilling.
- Bygg personvern inn i designet.
- Skap full funksjonalitet: både–og, ikke enten–eller.
- Ivareta informasjonssikkerhet fra start til slutt.
- Vær åpen om hvordan systemet fungerer, og hvordan personvern blir ivaretatt.
- Respekter brukerens personvern.

Eksempler på dette vil være at:

- Virksomheten gjør det enkelt å gi frivillig, informert samtykke og å trekke tilbake samtykket.
- Virksomheten gjør det mulig for personell å laste ned egen personopplysning via min side.
- Automatisert varsler om sletting av data som har utløpt.
- Begrense antallet personer som har tilgang til personopplysninger i interne systemer.
- Virksomheten bruker kryptering når de sender ekstern e-post og gjør det enkelt og sikkert å sende ut personopplysninger.
- Personopplysninger skal sikres mot uautorisert eller ulovlig tilgang og mot utilsiktet tap, ødeleggelse eller skade. Det skal settes i verk egnede tekniske og organisatoriske tiltak.

14.Etterkontroll og oppfølging

Forordningen krever at virksomheten organiseres på en måte som sikrer at regelverket etterleves. Dette kan ivaretas ved at det etableres faste rutiner for jevnlig etterkontroll og oppfølging. Rutiner og tiltak for etterkontroll og oppfølging tilpasses VIDs behandling av personopplysninger og den risikoen behandlingen representerer. Formålet er å sikre at virksomheten til enhver tid overholder forordningens krav. Virksomheten må kunne dokumentere hvilke rutiner for etterkontroll og oppfølging som er etablert, og de bør dermed beskrives i et samlet dokument.

Hjelpedokumenter: mal for egenkontroll fra Datatilsynet

Vedlegg: Liste over hjelpedokumenter

1. Beskrivelse om roller og ansvar i personvern i VID
2. Protokoll over behandlingsaktiviteter
3. Innsynsrutiner
4. Mal for samtykke som gjelder forskning, bilde video bruk osv.
5. Personvernerklæring, intervjuguide, samtykkeskjema, brev til de registrerte
6. Lagrings- og slettingsrutiner
7. Retningslinjer for ustrukturerte lagringsområder
8. Retningslinje for Informasjonssikkerhet
9. Mal for DPIA
10. Mal for protokoll
11. Mal for risikovurdering
12. Sikkerhetsinstruks for bruk av datasystemer
13. Mal for databehandleravtale
14. Roller og ansvar vedrørende signering/arkivering av databehandleravtale
15. Sjekkliste for databehandleravtalen fra Datatilsynet, veiledning fra Datatilsynet
16. Skjema for håndtering av avvik
17. Retningslinjer for klassifisering av informasjon
18. Mal for egenkontroll