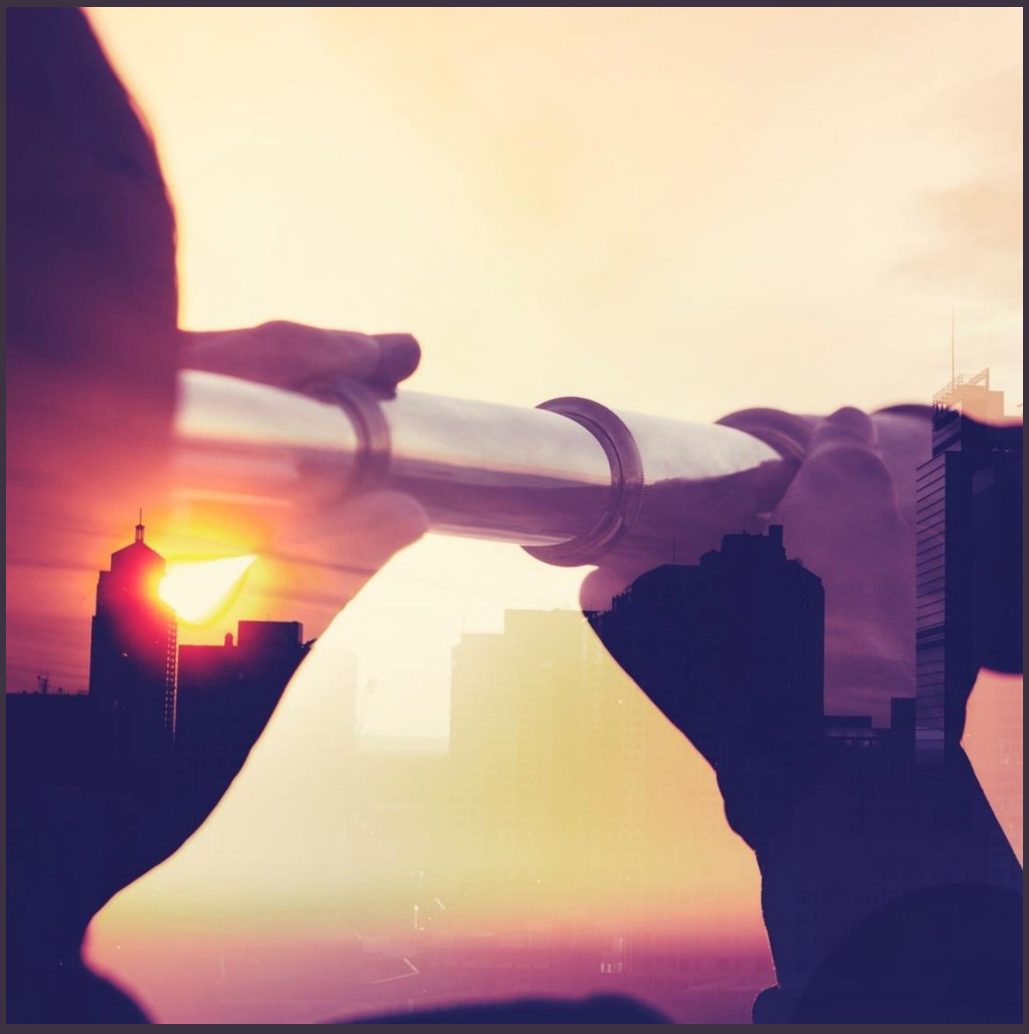
Energi Norge
Hele Norge på strøm



Bransjestandard – Personopplysningsloven

Forord

Alle deler av fornybarnæringen, både produsenter, nettvirksomhet og strømleverandører er berørt av krav til personvern. Overholdelse av personvernet er ikke bare et spørsmål om mulig straff, gebyrer, tvangsmulkter og erstatningsansvar. Det er også et spørsmål om omdømmet og tillit for en næring som gjennom digitalisering står foran store muligheter og utfordringer i møtet med kunden.

Godt personvern handler blant annet om å:

- Påse at grunnvilkår for behandling av opplysninger er oppfylt (kun behandling av personopplysninger til bestemte formål, kun der det foreligger hjemmel i lov, kundeavtale eller samtykke eller identifisert en berettiget interesse mv. samt oppfylle både nødvendighets- og relevanskrav).
- Ivareta den enkeltes rettigheter (tilstrekkelig informasjon slik at det er forutsigbare behandlinger, oppfylle innsynsrett ved begjæring om innsyn, vurdere og gjennomføre retting og sletting der vilkårene for dette er oppfylt mv.)
- Ivareta tilfredsstillende informasjonssikkerhet med hensyn til informasjonsverdiers konfidensialitet, integritet og tilgjengelighet.
- Sikre hensiktsmessige rutiner og andre tiltak for å oppfylle kravene, herunder opplæring og arbeid med sikkerhetskultur og prosesser for å legge til rette for kontinuerlig forbedring.

Denne bransjestandarden, med veiledning, er utviklet i samarbeid med våre medlemmer gjennom arbeidsmøter med et stort og representativt utvalg av medlemmer samt høringsrunder. EY har ledet dette arbeidet. Energi Norge vil gjerne takke alle som har bidratt i prosessen for alle nyttige innspill.

Dette dokumentet vil bli oppdatert jevnlig ved behov. Energi Norge setter pris på innspill og tilbakemeldinger om mulige forbedringsområder.

Energi Norge

Oslo 7.12.2020

Knut Kroepelien
Administrerende direktør

Dokumentrevisjon

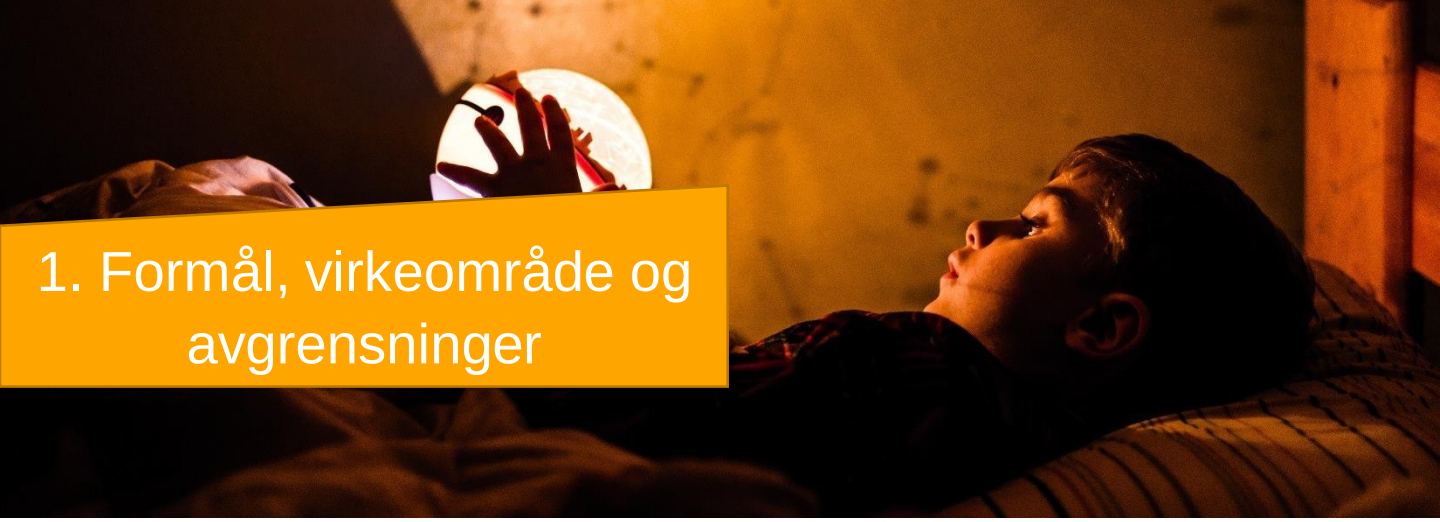
Versjons-nummer	Dato	Merknad
1.0	7.12.2020	Nyetablert bransjestandard personopplysningsloven

Forklaring på symbolbruk mv.

	Forklaring	Beskrivelser, definisjoner e.l.
	Krav	Oversikt over krav
	Eksempler	Eksempler på god praksis, hvordan krav skal forstås mv.
	Tips	Praktiske tips

Innholdsfortegnelse

Innholdsfortegnelse forts.



1. Formål, virkeområde og avgrensninger

1.1 Formålet med bransjestandarden

Fornybarnæringen skal utvikle og tilby tjenester av høy kvalitet samtidig som systemer, verktøy og prosesser ivaretar personvern i henhold til kravene i personopplysningsloven.

Formålet med denne bransjestandarden er å legge til rette for en harmonisert ivaretakelse av personvern blant aktørene i bransjen, slik at kunder og andre registrertes personverninteresser blir ivaretatt på en god og effektiv måte.

1.2 Virkeområde og avgrensninger

1.2.1 Virkeområde

Med behandling av personopplysninger menes enhver innsamling, registrering, strukturering, lagring, tilpasning, sammenstilling, bruk, oppslag i, utlevering, sletting eller annen behandling1 som omfattes av definisjonen i personvernforordningen.

Denne bransjestandarden retter seg mot behandling av personopplysninger om kunder og andre registrerte i virksomhetsområder underlagt energiloven. Dette vil si juridiske enheter som driver med produksjon, omforming, overføring, omsetning og fordeling av fornybar energi og andre aktører i verdikjeden, herunder enheter som Elhub. Den retter seg også mot virksomheter som understøtter slik virksomhet, som for eksempel leverandører og andre tjenesteytere. Bransjestandarden er også til bruk for det lokale elektrisitetstilsyn (DLE), sakkyndige selskaper og entreprenører som utfører oppgaver for nettselskap for strømforsyning. For andre aktører som eksempelvis fiberaktører, kan veileder og bransjestandard gjerne benyttes så langt den passer, men det er viktig at det da tas høyde for annen type særregulering som kan påvirke både hvilke krav som samlet sett gjelder og hvordan disse forventes å bli oppfylt. Dette er bl.a. aktuelt for virksomheter som er underlagt ekomlovgivningen.

Bransjestandarden består av dette dokumentet. I tillegg finnes det støttedokumenter som bl.a. mal for behandlingsoversikt, som er tilgjengelig via Energi Norges hjemmesider.

1. Se definisjonen i personvernforordningen artikkel § 4 nr. 2

1.2.2 Avgrensninger

Denne bransjestandarden gir ingen uttømmende veiledning av hvilke tiltak som er nødvendig å iverksette for å overholde personopplysningsloven og tilhørende forskrifter. Ved eventuell motstrid, går andre nasjonale og internasjonale rettslige forpliktelser foran innholdet i dette dokumentet.

For utførlig veiledning og tolkning av særskilt regelverk om markedsføring i lys av personvernregelverket, må virksomheten rådføre seg med Forbrukertilsynet og det veiledningsmateriell de har tilgjengelig. På enkelte punkter vil denne veilederen likevel gi noen eksempler knyttet til forhold som reguleres både av personopplysningsloven og markedsføringsloven.

Denne bransjestandarden omfatter ikke behandling av personopplysninger om ansatte.

1.2.3 Forholdet til annet regelverk, standarder mv

Det er ikke bare krav til ivaretakelse av personvern som krever at virksomheter har systematisk styring og kontroll for å etterleve krav, også energiloven, sikkerhetsloven, arbeidsmiljøloven, mv. krever implisitt eller eksplisitt at det etableres en internkontroll for å oppfylle kravene i de respektive lovene. Det vil kunne være betydelige overlapp mellom de tiltak som er nødvendig for å oppfylle slike krav. Det kan derfor være hensiktsmessig å vurdere hvilke områder det kan etableres og vedlikeholde et felles internkontrollsystem for. I tillegg kan det være nyttig å sikre god sammenheng mellom prosesser etter personopplysningsloven med andre prosesser i virksomhetsstyringen, som budsjettprosesser og andre rapporteringer til ledelsen.

Det finnes ulike standarder som er utviklet over tid for å legge til rette for hensiktsmessige tiltak og god styring, som for eksempel ISO-standarden 27001/2 om etablering av styringssystem for informasjonssikkerhet. Denne bransjestandarden gir imidlertid ingen anbefalinger om bruk av en bestemt eller flere standarder. Selv om en virksomhet tar utgangspunkt i en eller flere standarder, må virksomheten som selvstendig behandlingsansvarlig fortsatt ta stilling til hva som er nødvendig og tilstrekkelig for egen del etter konkrete vurderinger av risiko for egen virksomhet.

2. Formålsinndeling

Samlet sett i bransjen behandles det personopplysninger om nåværende, tidligere og kommende kunder, deres eventuelle fullmektig, anleggseiere, grunneiere samt kontaktpersoner hos installatører og elektroentreprenører. Denne veilederen og bransjestandarden omfatter følgende overordnede behandlingsformål for behandling av personopplysninger:

	Forklaring av behandlingsformål
Administrere kundeforhold	• Behandling av nødvendige personopplysninger i forbindelse med etablering av ny kunde, forvaltning av eksisterende kundeforhold, endring av strømavtaler, stenging av strøm som følge av manglende betaling samt opphør av kundeforholdet. • Dette omfatter også behandling av anmodning om fritak fra aktive kommunikasjonsmoduler til AMS-målere.
Måling, avregning, fakturering og innfordring	• Behandling av nødvendige personopplysninger i forbindelse med måleravlesing (Registrering og validering av målerverdier), fakturering ut fra forbruk, pris og betalingsavtale og innfordring, herunder inkasso.
Teknisk drift og kundestøtte	• Behandling av nødvendige personopplysninger i forbindelse med avbruddsregistrering og spenningsmåling, mottak av meldinger om jordfeil mv, befaringer, feilsøkeprosesser, feilretting på distribusjonsnettet og i strømforsyningen, varsling av utkobling/feil, fakturering av erstatningspliktig person eller firma som har skadet strømnettet.
Markedsføring mot eksisterende kunder og potensielle kunder	• Behandling av nødvendige personopplysninger i forbindelse med ønske om markedsføringsaktiviteter mot eksisterende kunder og potensielle nye kunder. • Den enkelte kunde anses som eksisterende kunde inntil leveranse av tjenester er opphørt og sluttfaktura for mottatte tjenester er betalt.
Internt forbedringsarbeid	• Analyse og innsiktsarbeid som metode kan blant annet omfatte statistiske analyser, utredninger og forskningslignende metoder for å få innsikt/kunnskap og erfaringer om egne ansvarsområder med sikte på forbedringer av for eksempel egne prosesser, mer effektiv utnyttelse av nettet mv. Dette kan i noen tilfeller anses som en del av de opprinnelige formål, eller som noe som går utover de øvrige formål, og dermed krever eget behandlingsgrunnlag. Dette må vurderes konkret.

Forklaring av behandlingsformål (forts)	
Det lokale El-tilsyn (DLE)	• Behandling av nødvendige personopplysninger i forbindelse med avtaler for gjennomføring av tilsyn, selve gjennomføringen og utarbeidelse av tilsynsrapporter.
Planlegge og bygge ut eller endre nettstruktur for strømnettet	• Behandling av nødvendige personopplysninger i forbindelse med planlegging og flytting eller utbygging av overføringsnett. • Dette innebærer kontakt og avklaringer med grunneiere, aktuelle kunder og koordinering med installatører samt eventuell erstatning til grunneier.
Internt forbedringsarbeid	• Analyse og innsiktsarbeid som metode kan blant annet omfatte statistiske analyser, utredninger og forskningslignende metoder for å få innsikt/kunnskap og erfaringer om egne ansvarsområder med sikte på forbedringer av for eksempel egne prosesser, mer effektiv utnyttelse av nettet mv. Dette kan i noen tilfeller anses som en del av de opprinnelige formål, eller som noe som går utover de øvrige formål, og dermed krever eget behandlingsgrunnlag. Dette må vurderes konkret.

Den enkelte virksomhet må selv vurdere hvorvidt disse formålsbeskrivelsene er dekkende for de behandlingsaktivitetene som utføres i virksomheten. Det samme gjelder for hvilket detaljeringsnivå innen hvert formål som er tilstrekkelig for å sikre egen etterlevelse gjennom tilpassede rutiner, hensiktsmessig internkontroll mv.

3. Kategorier av personopplysninger

Med personopplysninger menes alle opplysninger som enten direkte eller indirekte er egnet til å knytte de aktuelle opplysningene til identifiserbare enkeltpersoner, og må behandles og sikres deretter i tråd med krav til personvern.[2]

Til hvert av formålene nevnt under kapittel 3 behandles det flere typer personopplysninger. Oversikten nedenfor viser typiske eksempler på hva som er å anse som personopplysninger, og vi har her gruppert disse i ulike typer kategorier ut fra hva som kjennetegner disse. Dette er ikke en uttømmende liste, og det kan til dels være innbyrdes overlapp mellom kategoriene.

Kategorier og eksempler på innhold	
Identifikasjons-opplysninger	• Navn, fødselsnummer, kundenummer, organisasjonsnummer,[3] gårds- og bruksnummer, kontaktpersoner (verge mv), bankkontonummer, IP-adresse mv.
Kontaktinformasjon	• Adresser, epostadresse, telefonnummer mv.
Anleggsdata	• Målernummer, målepunkt-ID, anleggsnummer, målerverdier, komponenter/utstyr med unikt nummer, opplysninger som angir geografisk posisjon (koordinater, posisjonsdata mv).
Kundegenererte data	• Opplysninger fra måling, avregning, fakturering og betalingshistorikk som benyttes eller tilgjengeliggjøres på en slik måte at det er mulig å spore tilbake til hvilken kunde disse stammer fra, er også slike opplysninger å anse som personopplysninger og må behandles deretter. Dette gjelder selv om en slik oversikt ikke er direkte koblet til kundeopplysningene. For eksempel informasjon om betalingshistorikk, utestående saldo på en gitt dato eller strømforbruk.
Særlige kategorier	• Helseinformasjon[4] som for eksempel mottas i forbindelse med uoppfordret søknad om fritak fra installering av kommunikasjonsenhet i AMS-måleren[5] ved anmodning om betalingsutsettelse mv.

Alle virksomheter må selv vurdere om det i tillegg behandles andre opplysninger som enten alene eller sammenstilt, vil kunne identifisere enkeltindivider og dermed anses som personopplysninger. Det vil typisk være opplysninger som er av så unik karakter at den direkte eller indirekte kan være egnet til å spore tilbake til en enkeltperson selv om den aktuelle presentasjonen isolert sett ikke inneholder navn, kundenummer eller lignende.

[2] Personvernforordningen artikkel 4, pkt. 1)
[3] Om enkeltmannsforetak, bør det vurderes behandlet som personopplysninger
[4] Se kapittel 7 der det anbefales at slike opplysninger slettes etter at henvendelsen er vurdert
[5] Se beskrivelse i vedlegg 1

4. Krav om behandlingsgrunnlag

All behandling av personopplysninger krever et behandlingsgrunnlag.[6] For fornybarnæringen er de mest relevante hjemmel i lov og forskrift, avtale med kunde, samtykke eller såkalt berettiget interesse for den som er ansvarlig for behandlingen. Det finnes imidlertid flere alternative behandlingsgrunnlag i personvernforordningen som kan være aktuelle i visse situasjoner.

4.1 Lov/forskrift

Det er flere lover og forskrifter som pålegger bransjen oppgaver som innebærer behandling av personopplysninger, og som dermed vil være det rettslige grunnlaget for slike behandlinger. De mest sentrale av disse er:

- Lov om produksjon, omforming, overføring, omsetning, fordeling og bruk av energi m.m. (energiloven)
- Forskrift om måling, avregning, fakturering av nettjenester og elektrisk energi, nettselskapets nøytralitet mv.
- Forskrift om forebyggende sikkerhet og beredskap i energiforsyningen (beredskapsforskriften)
- Lov om forbrukerkjøp (forbrukerkjøpsloven)

I tillegg eksisterer det lover som pålegger bransjen å oppbevare personopplysninger etter nærmere bestemte frister, som vil være det rettslige grunnlaget for oppbevaring av personopplysninger også etter at et kundeforhold er avsluttet. De mest sentrale lovene er:

- Lov om foreldelse av fordringer (foreldelsesloven)
- Lov om bokføring (bokføringsloven)

Hver virksomhet må ha oversikt over de lovkrav som treffer egen virksomhet.

Det er en oversikt over mange av de aktuelle lover og forskrifter i bransjen på hjemmesiden til Energi Norge.

[6] *Se krav til behandlingsgrunnlag i personvernforordningen artikkel 6 til 10.*

4.2 Avtale med kunde

Når behandling av personopplysninger er nødvendig for å oppfylle en avtale med kunde, er dette tilstrekkelig behandlingsgrunnlag for den aktuelle behandlingen.[7]

Energi Norges standardavtaler for nettleie, tilknytning og kraftlevering regulerer den tjenesten som virksomheten hovedsakelig leverer til kunden og er et eksempel på bruk av avtaler innen fornybarnæringen.

Et annet eksempel på avtale er når kunden aktivt bestiller åpning av HAN-port. Egne avtaler kan videre omfatte andre energitjenester, utvidet energirapportering, laststyring (aggregatortjenester) som er tjenester utover det som er en del av produktet som kunden har valgt.

- Standardavtale og tilleggsvilkår kan kun brukes som behandlingsgrunnlag for aktiviteter som er nødvendige for å tilby den tjenesten som avtalen regulerer.
- Eventuelle tilleggstjenester som går utover tjenesten som standardavtalen og tilleggsvilkår hovedsakelig omhandler, må ha egne avtalevilkår som kunden må akseptere separat eller ha kundens samtykke som behandlingsgrunnlag.
- Avslutning av et kundeforhold på et gitt målepunkt-ID, innebærer terminering av alle aktuelle bestillinger og tillatelser for aktuell HAN-port, selv om disse ikke uttrykkelig termineres eller trekkes tilbake.

4.3 Samtykke

Behandlingsaktiviteter som ikke er nødvendige for å levere virksomhetens hovedtjeneste til kunden, vil normalt ha samtykke som behandlingsgrunnlag[8] med mindre det foreligger et annet gyldig behandlingsgrunnlag. Om samtykket trekkes tilbake, må aktuell behandling basert på samtykket, stanse.

- Ved innhenting av samtykke[9] må det påses at det er en frivillig, spesifikk, informert og utvetydig viljesytring fra vedkommende. Den må være gitt gjennom en erklæring eller en tydelig bekreftelse som innebærer at vedkommende gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende.
- Innhentes det samtykke samtidig som det inngås en kundeavtale, må samtykket være tydelig atskilt fra vilkår knyttet til inngåelse av kundeavtalen.
- Det skal gis forståelig og lett tilgjengelig informasjon på et klart og enkelt språk. Dette omfatter også informasjon om at samtykket kan trekkes tilbake.
- Det skal legges til rette for enkel tilbaketrekking.
- Det er den enkelte virksomhet som har bevisbyrden for at det foreligger et gyldig samtykke, et samtykke skal derfor fortrinnsvis gis skriftlig.

Eksempler på bruk av samtykke i bransjen:

- Bruk av HAN-port for andre aktører, for eksempel i forbindelse med megling eller rådgivning fra andre selskap.
- Tillatelse til utlevering av personopplysninger til andre enn de som har hjemmel i lov til å motta eller begjære utlevering av personopplysninger. Samtykket må i slike tilfeller være konkret på type personopplysninger og hvem det kan leveres ut til.
- Krav om samtykke til bruk av telefon ved direkte markedsføring.

[7] Personvernforordningen artikkel 6, pkt. 1) bokstav b)
[8] Samtykke er et mulig behandlingsgrunnlag jf. Personvernforordningen artikkel 6 pkt. 1
[9] Krav til samtykke følger av personvernforordningen artikkel 4 pkt. 11 og artikkel 7 Vilkår for samtykke, samt fortalepunkt 32) og 42). Krav til barns samtykke følger av Personopplysningsloven §5 og personvernforordningen artikkel 8. Artikkel 29-gruppen har skrevet retningslinjer for samtykke (WP259)

4.4 Berettiget interesse

En virksomhet kan behandle personopplysninger dersom det er nødvendig for å ivareta en berettiget interesse som veier tyngre enn hensynet til den enkeltes rettigheter og friheter.[10] For at en virksomhet skal kunne bruke slik berettiget interesse som behandlingsgrunnlag, må den berettigete interessen rent faktisk foreligge og det er ikke tilstrekkelig å bare påberope seg den. For å avklare hvorvidt interessen faktisk er berettiget, må virksomheten vurdere de ulike fordeler og ulemper for egen virksomhet og de registrerte opp mot hverandre. Denne vurderingen skal dokumenteres og må kunne fremvises både til den registrerte og til Datatilsynet på forespørsel.

Dette krever en avveiing av interesser mellom den behandlingsansvarlige og den registrerte. Det må alltid vurderes tiltak for å minimere personvernkonsekvensene. Det kan for eksempel være å gi adgang til å reservere seg, eksempelvis fra nyhetsbrev, invitasjoner til arrangementer eller lignende. Det er videre viktig å være klar over den enkeltes rett til å protestere mot behandlingen når berettiget interesse benyttes som behandlingsgrunnlag.[11]

- En berettiget interesse må være lovlig, klart definert i forkant av oppstart av behandlingen og være saklig begrunnet i virksomheten.
- Den aktuelle behandlingen av personopplysninger må være nødvendig for denne interessen.
- Det er videre et krav om å velge den behandlingen som er minst inngripende for personverninteressene til den enkelte.
- Deretter må virksomheten foreta en interesseavveining for å avgjøre om den enkeltes personvern veier tyngre enn virksomhetens berettigede interesse. En interesseavveining i den behandlingsansvarliges favør, må alltid dokumenteres.

Planlegging nettnytte mv for nettselskap:

- Bruk av innsamlede data fra målepunktet i kundens anlegg i nettselskapenes planlegging og drift av overføringsnettet, inklusive behovet for fremtidige utvidelser av strømnettet. Omtales ofte som «nettnytte».
- Virksomhetens interesse er å ivareta ansvaret for et fremtidsrettet, stabilt og økonomisk nett som kommer alle til gode.
- Samtidig anses personvernulempene for den enkelte som forholdsvis lav fordi det ikke er den enkeltes forbruk i seg selv som er det interessante å se nærmere på, men de aggregerte tall. Slike data anonymiseres om disse ønskes beholdt utover fastsatt lagringstid.

Eksempel – Nettselskapets kontakt med potensielle interessenter ved nyutbygging:

- Kontakt typisk mot nye hytteeiere for å avklare interesse for tilkobling.
- Kunden kan ha interesse av samlet utbygging av økonomiske hensyn.
- Slik kontakt kan også ses å være nærmere knyttet til samfunnsoppdraget og oppfyllelse av tilknytningsplikten enn mer typisk markedsføringsaktivitet for tjenester der selskaper konkurrerer om de samme kundene.
- Informasjon som benyttes for å identifisere aktuelle interessenter vil typisk være åpen informasjon eller informasjon den enkelte selv har gjort tilgjengelig.
- Viktige tiltak fra virksomhetens side i slike tilfeller for å minimere belastningen å sørge for god informasjon der det kommer tydelig frem at det er helt frivillig for den enkelte om de ønsker å melde interesse og bestille tilkobling.

[10] *Se Personvernforordningen artikkel 6, pkt. 1. Se også fortalepunkt 45*
[11] *Se Personvernforordningen artikkel 21*

Eksempel – Kontakt med ny eier ved anleggsovertakelser:

- Strømleverandørens kontakt med ny eier eller ny leietaker ved anleggsovertakelse for å legge til rette for kontinuitet i leveranse til målepunkt-ID. Alternativet vil være stenging av anlegget i en periode eller en situasjon med leveringsplikt.
- Dette innebærer at strømleverandør proaktivt kan ta kontakt med ny eier eller leier per telefon for å spørre om ønsker for videre leveranse. Dette forutsatt at kunden ikke har reservert seg mot telefonsalg.
- Personvernulempene for den enkelte anses å være forholdsvis liten ved slik kontakt fordi det ikke innebærer mer enn en forespørsel som kunden kan avslå.
- Tiltak på virksomhetens side må blant annet omfatte tilstrekkelig informasjon om frivillighet, konsekvenser av å ikke ønske leveranse mv.
- Informasjon om eventuell ny kunde sendes deretter til nettselskapet.
- Strømleverandør bør deretter slette opplysninger om antatt ny sluttbruker og avslutte saken.

Eksempel – Markering av kunder som fremstår som truende overfor nettselskapet:

- Markering av hvem som er truende kunder som krever tiltak ved fysisk stenging, målerbytte mm ute hos kunde. Dette er typisk personer som tidligere har fremsatt alvorlige trusler eller opptrådt truende ved lokalt oppmøte i forbindelse med stenging av anlegg som følge av manglende betaling eller lignende. I slike tilfeller kan det av hensyn til sikkerheten til utsendt mannskap være nødvendig å være flere på oppdraget samt avtale en beredskap med lokalt politi. Det samme kan være aktuelt for et kundesenter som har kundemottak.
- Hensyn til helse, miljø og sikkerhet for å sikre de ansattes interesser, vil alltid veie tungt i virksomheters favør.
- For kunden kan imidlertid dette oppleves som et inngripende og stigmatiserende tiltak. Det er derfor viktig at slik markering bare er tilgjengelig eller kjent for de som har et tjenstlig behov for slik informasjon og ikke inngår i felter som utveksles med andre aktører i bransjen, som for eksempel Elhub. Videre må det foreligge en rutine for revurdering av slike koder slik at disse ikke henger igjen over tid uten at det foreligger et saklig behov for det.

5. Fordeling av roller og ansvar

En virksomhet må ha oversikt over hva som er egen rolle i ulike prosesser og tjenester i alle verdikjeder. Det vil si om virksomheten er:

- Behandlingsansvarlig[12] for aktuell behandling,
- En databehandler[13] som behandler personopplysninger på vegne av en annen virksomhet, eller
- En leverandør som kun leverer systemstøtte e.l. som benyttes av de ansvarlige virksomheter i deres behandling av personinformasjon, og uten tilgang til aktuelle personopplysninger.

Hvilken rolle virksomheten innehar, er avgjørende for hvilke plikter virksomheten har. Både den behandlingsansvarlige og en databehandler har en rekke lovbestemte plikter, i tillegg til det som måtte reguleres gjennom avtale mellom partene. Det er den behandlingsansvarlige som har totalansvaret, herunder ansvar for å påse at krav i databehandleravtaler er tilstrekkelig presise, samt følge opp både databehandlers og leverandørers utførelse av oppdraget.[14] Om flere aktører deltar i deling eller bearbeiding av personopplysninger i en verdikjede, må det dermed klargjøres hvem er behandlingsansvarlig for hva.

Om flere virksomheter sammen bestemmer formål og virkemidler ved en behandling, kan det foreligge et delt eller felles behandlingsansvar. I slike tilfeller er det også behov for en skriftlig avtale som fastsetter rolle- og ansvarsfordeling. Dette er imidlertid ikke en databehandlerrelasjon ettersom ingen av partene behandler personopplysninger på vegne av den andre. I slike tilfeller skal det derfor ikke inngås en databehandleravtale.

En virksomhet må ha oversikt over hva som er egen rolle i ulike prosesser og tjenester i alle verdikjeder.

Eksempler på databehandlere:

- Drifts- eller systemleverandør som har tilgang til personinformasjon
- Leverandør av tjenester fra callsenter for salg av egne produkter

[12] Definisjonen av en behandlingsansvarlig følger av Personvernforordningen artikkel 4 pkt.7. Se forøvrig artikkel 28 om krav til behandlingsansvarlig.
[13] Definisjonen av en databehandler følger av Personvernforordningen artikkel 4 pkt. 8. Krav til databehandlere følger av artikkel 28.
[14] Den behandlingsansvarliges ansvar følger av personvernforordningen artikkel 24.

Behandlingsansvarlig eller databehandler? Noen ganger kan det oppstå tvil om hvem som har hvilken rolle. Noen kontrollspørsmål som kan hjelpe til å sortere i den forbindelse er:

- Hvem bestemmer formålet?
- Hvem er det som bestemmer at det skal samles inn personopplysninger i utgangspunktet?
- Hva er det juridiske grunnlaget for å behandle personopplysninger?
- Hvem bestemmer hvilke personopplysninger som skal samles, hvilke individer det skal samle inn data om?
- Hvem tar stilling til om det eventuelt skal leveres ut data og til hvem?
- Hvem vurderer og beslutter hvor lenge dataene skal lagres?
- Kan begge aktører kreve innsyn eller tilgang i alle personopplysninger som behandles om en enkeltperson?

5.1 Internt i virksomheten

Ansvaret for at krav til behandling av personopplysninger er ivaretatt, tilligger øverste leder i den virksomheten som bestemmer bruk av personopplysninger og elektronisk behandling av disse. Dette innebærer å sørge for at virksomheten ivaretar alle plikter som påhviler den, herunder å iverksette egnede tekniske og organisatoriske tiltak som både skal sikre og dokumentere at behandlingen av personopplysninger skjer i samsvar med kravene i personopplysningsloven. Ledelsen må sette av tilstrekkelig ressurser slik at kravene håndteres på en god måte. Det innebærer bl.a. at rolle- og ansvarsfordelingen internt i virksomheten må klargjøres og dokumenteres. Delegering av slike oppgaver bør knyttes til lederstillinger slik at det foreligger reell innflytelse på behandlingene.

Uavhengig av størrelsen på virksomheten, må oppgaver fordeles på flere. Dette vil typisk innebære å fastsette hva som ligger i linjeansvar og hva som tilligger spesielle nøkkelroller som for eksempel prosesseier, produkteier, systemeier, systemansvarlig, IT-ansvarlig, HR-ansvarlig mv. Samtidig kan det være en stor fordel å ha en bestemt person/enhet med særlig kompetanse å henvende seg til med spørsmål rundt behandling av personopplysninger og som kan koordinere internt, slik at praksis ikke blir unødig forskjellig mellom de ulike avdelinger/enheter i virksomheten.

Rolle- og ansvarsfordelingen internt i virksomheten må klargjøres og dokumenteres.

Det er flere måter å dokumentere fordeling av roller og ansvar på[15]

- Noen virksomheter velger å lage rolle- og ansvarsmatriser, andre lister opp ulike roller med tilhørende ansvar i kulepunkter samt oppdaterer stillingsinstrukser, mens andre foretrekker visuelle fremstillinger og markering på foreliggende prosess- og organisasjonskart.

Selskaper i et konsern som består av flere datterselskaper må påse at eget ansvar for etterlevelse av krav til personvern og eventuelle bestemmelser om taushetsplikt eller annen begrensning i deling av opplysninger på tvers, blir ivaretatt der felles konsernenhet eller andre fellesfunksjoner påtar seg oppgaver på vegne av flere av selskapene.

5.2 Utnevning av personvernombud og innhold i rollen

Sentrale oppgaver for personvernombudet[16] vil være å påse samt bistå til oversikt over behandlinger, veilede virksomheten i ivaretakelse av kravene, bistå i opplæring internt i virksomheten og i behandling av klager fra både virksomhetens egne ansatte og eksterne aktører relatert til bruk av personopplysninger.[17] Et personvernombud skal ha en uavhengig rolle. Personvernombudet skal ha mulighet til å rapportere direkte til øverste ledelse.[18]

En virksomhet kan i tillegg legge flere oppgaver til personvernombudet enn det som er regulert i lovteksten.

Selv om det utnevnes et personvernombud, er det fortsatt den behandlingsansvarlige som er ansvarlig for at behandlingen av personopplysninger skjer i tråd med regelverket.

Det er den enkelte virksomhet som selv må vurdere om egen virksomhet er av en slik karakter at det utløser en plikt til å ha personvernombud.

For en del virksomheter er det nå obligatorisk å ha personvernombud. Dette gjelder bl.a.:[19]

- Offentlig myndighet/offentlig organer,
- Der hovedvirksomheten består av aktiviteter som på grunn av sin art, sitt omfang og/eller formål krever regelmessig og systematisk monitorering i stor skala

Virksomheter i fornybarbnæringen anses per i dag ikke å ha plikt til å utnevne personvernombud.[20] Dette kan imidlertid endre seg. Enten som følge av fremtidig lov- eller forskriftsendringer, klargjøring fra datatilsynsmyndighetene eller som følge av at virksomheten etablerer nye produkter eller på annen måte endrer på egen oppgaveløsning og dermed hvordan personopplysninger behandles. Ved slike omstendigheter, må spørsmålet om plikt til å ha personvernombud, vurderes på ny.

Dette er argumentene for hvorfor det ikke anses å foreligge en plikt til å utnevne personvernombud i fornybarnæringen per i dag:

- Fornybarnæringen utfører ikke behandlinger som offentlig myndighet eller som et offentlig organ som omfattes av forvaltningslovens § 1.[21] Nettselskapets DLE-rolle alene utløser heller ikke krav om personvernombud for hele nettselskapet og de øvrige tjenestene, da dette utgjør en så vidt liten del av det samlede omfanget av behandling av personopplysninger.
- Fornybarbransjen anses ikke å ha kjernevirksomhet i form av behandlingsaktiviteter som på grunn av sin art, sitt omfang og/eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte.[22] [23]

[15] HUKI eller RACI-matriser er aktuelle eksempler, se bl.a.: https://en.wikipedia.org/wiki/Responsibility_assignment_matrix
[16] Krav til personvernombud og personvernombudets oppgaver følger av Personopplysningsloven §§ 9, 10 og 11, samt Personvernforordningen artikkel 37, 38 og 39
[17] Personvernforordningen artikkel 38 og 39
[18] Personvernforordningen artikkel 38 pkt. 3
[19] Personvernforordningen artikkel 37
[20] Personvernforordningen artikkel 37
[21] Personvernforordningen artikkel 37 nr. 1 bokstav a
[22] Personvernforordningen artikkel 37 nr. 1 bokstav b
[23] Artikkel 29-gruppen, nevner uttrykkelig under omtalen av alternativ a at de anbefaler energibransjen å ha personvernombud uten at dette er pliktig under alternativ a. En slik anbefaling ville vært unaturlig, dersom virksomhetene likevel plikter å ha personvernombud etter alternativ b. Se «Guidelines on Data Protection Officers ('DPOs')» s. 6. Se forklaring på artikkel 29-gruppen i Vedlegg 1)

- Ved installasjon av smart strømmåler og detaljert strømforbruk kan forbruket og variasjon i forbruket spores tilbake til en bestemt abonnent eller gruppe av abonnenter knyttet til det aktuelle målernummeret i en bestemt periode. I tillegg kan slike målere gi nettselskapene informasjon om strømbrudd, jordfeil eller problemer med spenningskvaliteteten.
- Disse behandlingene skjer først og fremst for faktureringsformål, eller for øvrig som ledd i å understøtte drift og forvaltning av strømnett, noe som må regnes som en nødvendig støttefunksjoner og det skjer ingen systematisk monitorering i den hensikt å følge med på forbruk. Mer detaljert informasjon via smarte strømmålere om en gruppe eller et enkeltindivid enn tidligere, er ikke egnet til å utlede annet enn antakelser om personkretsen tilknyttet det aktuelle målernummeret. Personkretsen kan dessuten være både en enkeltperson og en større gruppe personer.

Utnevnelse av personvernombud på frivillig basis

En virksomhet kan velge å utnevne personvernombud på frivillig basis. De samme kravene som gjelder for den som er pliktig å ha personvernombud, vil da gjelde, med mindre man i et slikt tilfelle velger etablere og navngi en funksjon som personvernkoordinator e.l. i stedet.

Ved vurdering av etablering av et personvernombud på frivillig basis, er det bl.a. naturlig å se hen til virksomhetens størrelse, organisasjonsmodell, kompleksitet, egen modenhet, organisering av ivaretakelse av personvern for øvrig, og om det er ønskelig å benytte en slik utnevnelse til å demonstrere for omverden at virksomheten tar personvern på alvor.

Dele personvernombud på tvers i et konsern

Det er adgang til å dele personvernombud på tvers i et konsern, så fremt kravet om enkel tilgang til vedkommende og krav om uavhengighet blir overholdt.[24] Det må i slike tilfeller gjøres en vurdering av om konsernets samlede størrelse, struktur eller virkeområde gjør det forsvarlig og overkommelig å ha kun ett personvernombud. Det må også vurderes om det er andre forhold, for eksempel geografiske forhold, kombinasjonen av oppgaver eller annet, som vil kunne vanskeliggjøre en reell ivaretakelse av rollen.

[24] Se personvernforordningen artikkel 37 nr 2

Tips til rollebeskrivelse for personvernombud:

Personvernombudet skal bistå den behandlingsansvarlige i arbeidet med å ivareta krav til personvern etter personvernlovgivningen. Personvernombudet har en sentral, rådgivende, rapporterende og kontrollerende rolle i organisasjonen knyttet til ivaretakelse av personverninteresser og krav.

Personvernombudet har en uavhengig rolle og kan ikke motta instrukser om utførelsen av oppgavene sine eller inneha oppgaver som kommer i interessekonflikt med oppgaven som personvernombud.

Personvernombudet kan ikke straffes eller avskjediges for utførelsen av sine oppgaver.

Sentrale oppgaver[25] for personvernombudet er:

- Bidra til og påse at virksomheten har en oversikt over all behandling av personopplysninger.
- Bistå avdelinger og andre med konkret rådgivning i forbindelse med ivaretakelse av personvern og informasjonssikkerhet innen avdelingenes ansvarsområder, herunder ved anskaffelse, utvikling og ved andre endringer av informasjonssystemer og prosesser. Dette omfatter også å bli kontaktet for rådføring om vurdering av personvernkonsekvenser og valg av metode.
- Kontrollere gjennomføringen av personvernkonsekvensvurderinger.
- Kontrollere etterlevelsen av behandlinger av personopplysninger, herunder at det er etablert et system for internkontroll som vedlikeholdes.
- Gjennomføre holdningsskapende aktiviteter, opplæring mv.
- Motta og besvare henvendelser fra de registrerte herunder ansatte om behandling av personopplysninger, bistå med å ivareta deres personvernrettigheter.
- Bli involvert og rådgi i avvikshåndtering, ha oversikt over avviksmeldinger og eventuelt melde avvik til Datatilsynet.
- Påpeke brudd på reglene for behandling av personopplysninger og ved behov varsle ledelsen om enkeltbrudd.
- Foreta undersøkelser på forespørsel fra Datatilsynet og være Datatilsynets kontaktperson i kontakt med virksomheten, herunder koordinere kommunikasjon om brudd på regelverk og andre avvik mellom tilsynet og virksomheten. Dette omfatter også ansvar for å fasilitere forhåndskonsultasjoner med Datatilsynet.
- Holde seg orientert om utviklingen innen personvern gjennom opprettholdelse av dybdekunnskap, deltakelse i egnede fora mv.
- Rett og plikt til å rapportere til virksomhetens øverste ledelse. Dette omfatter både gjennom regelmessig oppsummering av status og ved uenighet i veivalg i enkeltsaker.
- Ivareta taushetsplikten som tilligger rollen som personvernombud etter personvernregelverkets bestemmelser.

[25] *Se Personvernforordningen artikkel 39, Personopplysningsloven §§8, 9 og 10.*

5.3 Eksternt: Roller og ansvar mellom aktører i verdikjeden

En databehandler er en aktør som behandler personopplysninger på vegne av den behandlingsansvarlige.[26] Det skal i slike tilfeller inngås databehandleravtaler som stiller krav til ivaretakelse av personvern og informasjonssikkerhet i leverandørens oppgaveløsning[27], se nærmere omtale i kapittel 13.

Eksempler på databehandleroppdrag for nettselskap:

- Nettselskapenes bruk av sakkyndige virksomheter for oppgaver innen det lokale eltilsyn (DLE) samt elektroentreprenører for anleggsarbeid mot sluttkunder, måler- og spenningskontroll mm.
- Systemleverandører som utvikler og/eller drifter kundeinformasjonssystemer for virksomhetene (KIS-leverandører)

Eksempel på deling av personopplysninger som ikke innebærer et databehandleroppdrag:

- Aktørene i bransjen som nettselskap, strømleverandør og Elhub er alle selvstendige behandlingsansvarlige for all behandling av personopplysninger som skjer i regi av egen virksomhet. Dermed er det ikke behov for noen databehandleravtale for deling av informasjon. Slik deling må ha tilstrekkelig behandlingsgrunnlag i lov, avtale eller samtykke, se kapittel 5.
- Inkassoselskap i rollen som inkassator iht. inkassoloven anses også som selvstendig behandlingsansvarlig.[28]
- Ved gjennomfakturering gir nettselskap fullmakt til strømleverandør til å opptre som nettselskapets representant for mottak av betaling av nettleie.[29] Dette er en fullmakt som regulerer det økonomiske forholdet mellom aktørene. Fullmakten har imidlertid ikke betydning for rekkevidden av aktørenes behandlingsansvar for egen behandling av personopplysninger, og den etablerer ikke en databehandlerrelasjon. Gjennomfaktureringen er basert på informasjon som omsetningsselskapet uansett er i besittelse av. Avregningsforskriften pålegger ikke noen ytterligere informasjonsflyt mellom nettselskap og strømleverandør, som for eksempel informasjon til nettselskapet om en kundes betalingsmislighold.
- Elektroentreprenører som opptrer på vegne av en kunde, er kundens leverandør, og opptrer på dennes vegne, og er ikke en databehandler på vegne av virksomheten. At virksomheten tilgjengeliggjør informasjon om kunden direkte til kundens elektroentreprenør, endrer ikke på dette.

[26] Se personvernforordningen artikkel 4, pkt. 8.
[27] Se personvernforordningen artikkel 28 pkt. 3.
[28] Se beskrivelse i Personvern i finanssektoren, Blixrud og Ottesen, side 423-425 og Datatilsynets vurdering i DT 05/01582
[29] Se avregningsforskriften om avtale om gjennomfakturering.

6. Oppbevaring og sletting

Personopplysninger skal slettes når formålet er oppfylt, med mindre det foreligger en oppbevaringsrett eller -plikt.[30] Slik rett eller plikt vil typisk følge av lov. Det er et flere generelle og bransjespesifikke bestemmelser[31] som har konkrete føringer for periode for oppbevaringsrett, -plikt eller på annen måte påvirker minimum eller maksimum oppbevaringstid for ulike typer personopplysninger. Dette handler typisk om plikt til oppbevaring for å gi mulighet for å utøve kontroll av økonomiske forhold fra myndighetenes side samt ivareta muligheten for å korrigere tilbake i tid der kunden urettmessige er avkrevd for mye for leveranser.

- Det skal fastsettes hvilke krav som gir føringer for oppbevaring og hva som er virksomhetens oppbevaringsbehov for alle personopplysninger. Begrunnelse skal dokumenteres.
- Det kan være aktuelt å beholde personopplysningene i opptil 3 år etter et skjæringspunkt som opphør av kundeavtale e.l. Dette som følge av den alminnelige foreldelsesfrist på 3 år eller utvidet foreldelsesfrist på 10 år. Dette vil for mange av personopplysningene i bransjen gi en samlet oppbevaringstid på 13 år.
- Opplysninger som ikke er relevante for kontroll og korrigeringsformål, skal slettes tidligere i forbindelse med opphør av kundeforhold.
- Opplysninger som kun oppbevares av hensyn til kontroll- og korrigeringsformål, underlegges strengere tilgangsstyring enn øvrige opplysninger når det opprinnelige formålet er oppnådd.
- Når lovlig oppbevaringstid er passert, enten fordi formålet er oppnådd eller maksimal tillatt oppbevaringstid bestemt i lov eller forskrift er passert, skal opplysningene slettes eller anonymiseres.
- Sletting krever fysisk tilintetgjørelse med mindre opplysningene reelt sett blir anonymisert.
    - Dette gjelder også for back-up. Unntak fra back-up kan gjøres, såfremt virksomheten har mekanismer som sikrer at ved behov for bruk av back-up, foretar vask mot informasjon som er slettet i produksjon, før back-up tas i bruk.
    - Dokumenter inneholdende personopplysninger skal sikkerhetsmakuleres på forsvarlig måte.
- For å sikre at slettefristene overholdes, skal alle virksomheter ha rutiner for sletting av opplysninger i alle databaser, filer o.l. hvor Personopplysninger lagres.

[30] Personvernforordningen artikkel 5, pkt. 1 bokstav e). Se også den registrertes rett til sletting i personvernforordningen artikkel 17.
[31] Energi Norge har på sin hjemmeside en oversikt over de mest sentrale lover og forskrifter.

Det må gjøres en konkret vurdering av relevante krav som treffer den aktuelle behandlingen, ofte knyttet opp til handlinger som f.eks. <x antall> <tidsangivelse> etter en inntrådt hendelse som f.eks. opphør av en kundeavtale eller lignende.

Veiledende føringer for fornybarnæringen:		
Kategorier	**Eksempler på innhold**	**Oppbevaringstid**
Identifikasjons-opplysninger	Navn, fødselsnummer, kundenummer, organisasjonsnummer[32], kontaktpersoner (verge mv), bankkontonummer, IP-adresse	Oppbevares så lenge forbrukeren har forpliktelser eller rettigheter ovenfor strømleverandør og nettselskap. Dersom forbrukeren har sagt opp både kraft- og nettleieavtale vil opplysningene lagres i ytterligere 10 + 3 år i tilfelle eventuelle feil og mulighet for å korrigere økonomiske oppgjør.
Kontakt-informasjon	Adresser, epostadresse, telefonnummer mv.	Oppbevares så lenge forbrukeren har en forpliktelser eller rettigheter ovenfor strømleverandør og nettselskap for strøm. Dersom forbrukeren har sagt opp både strøm- og nettleieavtale vil opplysningene lagres i ytterligere 10 + 3 år i tilfelle eventuelle feil og mulighet for å korrigere økonomiske oppgjør. Kontaktinformasjon i form av adresse, telefonnummer mv. kan kunden be om slettes tidligere.
Anleggsdata	Målernummer, målepunkt-ID, anleggsnummer, målerverdier, komponenter/utstyr med unikt nummer, geolokasjon.	Koblingen mellom anleggsdata og den enkelte som er registrert vil bli oppbevart så lenge forbrukeren har en forpliktelser eller rettigheter ovenfor strømleverandør og nettselskap, men ikke mer enn 10 + 3 år tilbake i tid. Dersom forbrukeren har sagt opp både strøm- og nettleieavtale, vil opplysningene lagres i 10 + 3 år i tilfelle eventuelle feil og mulighet for å korrigere økonomiske oppgjør.
Særlige kategorier	Helseinformasjon som mottas i forbindelse med søknad om fritak fra installering av kommunikasjonsmodul i AMS-målere.	Helseopplysninger oppbevares ikke etter at søknad er behandlet. Om klage på avslag eller vedkommende på et senere tidspunkt er i en endret situasjon, må kunde søke og fremlegge dokumentasjon på ny.

[32] *Om enkeltmannsforetak, bør det vurderes behandlet som personopplysninger.*

7. Rettigheter for den registrerte

7.1 Krav til informasjon

Kunden og andre det behandles personopplysninger om, skal uoppfordret gis informasjon om virksomhetens behandling av opplysninger på tidspunktet for innsamlingen av opplysningene.[33]

Den som er registrert skal få informasjon om identiteten og kontaktopplysninger til den behandlingsansvarlige og til et eventuelt personvernombud. I tillegg skal det informeres om hva som er formålet med behandlingen, aktuelt behandlingsgrunnlag, hvilke informasjonselementer som innhentes og fra hvilke kilder, eventuell utlevering og overføring av opplysningene, varigheten av behandlingen og den registrertes rett til innsyn, retting, sletting og øvrige rettigheter, herunder begrensning, portering mv, om det forekommer automatiserte avgjørelser, eventuell profilering, samt muligheten for å klage. Informasjonen må gis på en slik måte at den enkelte forstår hva behandlingene innebærer og dermed settes i stand til å ivareta egne rettigheter.

Informasjonen samles i en personvernerklæring eller tilgjengeliggjøres på annen måte, og den skal være kortfattet og lett å forstå for den registrerte slik at den skaper transparens og forutsigbarhet om hvordan opplysninger behandles. Kundeavtaler må enten ha informasjon i selve avtalen eller ha henvisning til hvor utfyllende informasjon er tilgjengelig. Den enkelte kan kreve at den behandlingsansvarlige utdyper informasjonen i den grad dette er nødvendig for å vareta egne interesser. Dette innebærer for eksempel spørsmål om oppbevaringstid eller hvordan informasjonen er sikret.

Unntak fra informasjonsplikten foreligger der den enkelte allerede har fått den aktuelle informasjonen. I tillegg er det visse andre unntak der det samles inn informasjon fra andre, for eksempel der innsamlingen er fastsatt i lov.[34]

Informasjon til registrerte om behandlinger virksomheten foretar skal inneholde følgende:[35]

- Formålet med behandlingen
- Beskrivelser av hvilke typer personopplysninger som behandles
- Hva som er behandlingsgrunnlaget
- Hvor opplysningene er hentet fra
- Om det er frivillig å avgi opplysninger
- Om personopplysningene vil bli utlevert, og eventuelt hvem som er mottaker
- Lagringstid
- Rett til innsyn i egne opplysninger og øvrige rettigheter
- Om det foregår en automatisert behandling og/eller profilering
- Navn og adresse på den behandlingsansvarlige og dennes eventuelle representant
- Kontaktinformasjon til personvernombudet, om virksomheten har det

[33] Se personvernforordningen artikkel 13 og 14
[34] Unntak fra retten til informasjon følger av personopplysningsloven §16, 1. ledd

Oppfyllelse av informasjonsplikten stiller krav til presisjon og klar kommunikasjon som den enkelte faktisk forstår. Det kan dermed være hensiktsmessig å dele opp informasjonstekster slik at man først gjør rede for hovedtrekkene, samtidig som det gis anvisning på hvor det er mer informasjon å finne for den som ønsker det.

7.2 Den registrertes innsynsrett

7.2.1 Innsynsretten[36]

Bestemmelser om innsynsrett i personopplysningsloven er gitt for å gi forutsigbarhet for den enkelte og sette vedkommende bedre i stand til å ivareta egne rettigheter.[37]

- Den registrerte har krav på innsyn i alle opplysninger som behandles om vedkommende. Dette gjelder uavhengig av i hvilke systemer eller hvordan opplysningene er lagret.
- Innsynsretten omfatter også personopplysninger som kun finnes i interne dokumenter, i logger eller på annen måte er registrert for interne formål, med mindre de faller inn under unntak fra innsynsretten gitt i norsk rett.[38]

- Innsyn skal gis i alle opplysningstyper som er registrert og alle formål opplysningene benyttes til. Det er likevel tilstrekkelig å hente frem kopi av samme opplysningstype én gang, selv om det er flere forekomster av samme opplysningstype.
- Rutiner på området skal ivareta den enkeltes interesser, men også bidra til at oppfølgingen av slike henvendelser kan skje effektivt. Med mindre det er et stort omfang av slike henvendelser, kan det være hensiktsmessig å sentralisere behandlingen av begjæring av innsyn.
- Innsyn kan etter nærmere avtale med den som ber om innsynet, avgrenses til de mest relevante opplysninger, f.eks. en eller flere bestemte typer personopplysninger eller formål som er registrert, til en nærmere avgrenset tidsperiode, eller på annen måte.
- Innsynet kan også gis i flere etapper så fremt den som begjærer innsynsrett gjøres oppmerksom på det og enkelt kan be om ytterligere informasjon. Dette er særlig praktisk der noen personopplysninger allerede er eller lett kan gjøres tilgjengelig via kundens egne sider mens øvrige personopplysninger må sammenstilles og utleveres på annen måte gjennom mer manuell sammenstilling.

[35] *Personvernforordningen artikkel 13 og 14*
[36] *Se personvernforordningen artikkel 15*
[37] *Se personvernforordningen fortalepunkt 59, 63 og 68*
[38] *Unntak fra den registrertes rett til innsyn følger av personopplysningsloven § 16, 1. ledd*

7.2.2 Avgrensning av innsynsretten[39]

Det kan i visse tilfeller gjøres unntak fra innsynsretten.

Det gis ikke innsyn i:

- Personopplysninger som det er påkrevd å hemmeligholde av hensyn til forebygging, etterforskning, avsløring og rettslig forfølging av straffbare handlinger,[40]
- Personopplysninger som utelukkende finnes i tekst som er utarbeidet for intern saksforberedelse, og som heller ikke er utlevert til andre, så langt det er nødvendig å nekte innsyn for å sikre forsvarlige interne avgjørelsesprosesser,[41]
- Personopplysninger som er underlagt taushetsplikt i lov eller med hjemmel i lov,[42]
- logger som viser hvem som har gjort oppslag i personopplysninger om den enkelte.[43]

7.2.3 Rutiner for innsyn

Rutiner skal bidra til å sikre at kun den som det er registrert opplysninger om, får utlevert disse ved begjæring om innsyn.

Krav til rutiner for innsyn:

- Personen som begjærer innsyn skal kunne identifiseres som den registrerte. Det innebærer at vedkommende må fremlegge gyldig identifikasjon ved personlig oppmøte eller annen metode som innebærer at man sikrer at personen er den vedkommende utgir seg for å være. Det kan for eksempel være autentisering av allerede etablert to-faktor autentisering eller ved bruk av Bank-ID via etablert innsynsportal.
- Foreligger ikke tilstrekkelig autentisering ved henvendelsen fra den registrerte, må metode for forsendelse sikre at det er rette vedkommende som mottar personopplysningene.
- Svaret sendes per post til den folkeregistrerte adressen, og skal aldri sendes per e-post uten tilstrekkelig sikringsmekanismer. Innsyn kan alternativt skje elektronisk, for eksempel via en "Min Side» eller annen type kundeportal såfremt autentiseringsmekanismer og andre sikringsmekanismer anses tilfredsstillende for aktuell type informasjon og aktuell risiko. For innsyn i egne opplysninger som samtidig er underlagt taushetsplikt, utgjør bruk av to-faktor autentisering minimumsnivå.
- Virksomheten må følge særskilte rutiner for personer med høyt beskyttelsesnivå, som er etablert for personer med adressesperre av type Strengt fortrolig og fortrolig – se omtale under kapittel 9.
- Innsyn skal gis uten ugrunnet opphold og senest innen 30 dager.[44] Dersom det vil ta lengre tid enn dette, skal det gis et foreløpig svar med opplysninger om grunnen til forsinkelsen og sannsynlig tidspunkt for når svar kan forventes.
- Om innsyn avslås, skal dette begrunnes skriftlig med presis henvendelse til unntakshjemmelen. Om det er personopplysningsloven § 16 første ledd bokstav f, må også aktuelle hensyn som tilsier hemmelighold, angis.

[39] Unntak fra retten til innsyn følger av personopplysningsloven §16
[40] Se personopplysningsloven § 16 1. ledd bokstav b
[41] Se personopplysningsloven § 16 1. ledd bokstav e
[42] Se personopplysningsloven § 16 1. ledd bokstav d
[43] Slik plikt krever mer presis hjemmel i lov eller en beslutning om å tilgjengeliggjøre slik informasjon av eget tiltak
[44] Personvernforordningen artikkel 12 pkt. 3 og fortalepunkt 59

7.3 Retting

Hovedformålet med retting[45] er å sørge for at virksomheten har oppdatert og korrekt informasjon om den aktuelle personen. Det er den som ber om retting som må sannsynliggjøre at opplysningene er uriktige og hva som er korrekt. Virksomheten bør likevel så langt som mulig bidra i å oppklare hva som er korrekt.

- Virksomheten plikter å rette feilaktige eller mangelfulle opplysninger om den registrerte. Virksomheten har plikt til uoppfordret å sørge for at opplysninger som behandles er riktige, herunder at det foretas nødvendig oppdatering og retting av opplysningene.
- Ved tvil om riktigheten av opplysningene bør de kontrolleres nærmere, for eksempel ved at den det gjelder eller opprinnelig kilde til de aktuelle opplysningene, kontaktes. Ved henvendelse fra den berørte skal retting skje så snart som mulig, med mindre virksomheten har grunn til å betvile at henvendelsen kommer fra rette vedkommende eller at det som opplyses, faktisk er korrekt.
- Retting innebærer vanligvis at uriktige opplysninger slettes og de korrekte settes inn, med mindre det er viktig å kunne dokumentere behandlinger gjort på bakgrunn av de uriktige opplysningene. Oppdatering skjer i tilfelle på den måten at opplysningene tydelig markeres og suppleres med korrekte opplysninger.
- Er feilen en feil i folkeregisteret eller Brønnøysundregistrene, må den registrerte henvises til å be om å få rettet feilen der. Det samme gjelder feil i opplysninger registrert hos kraftomsetter som andre aktører baserer seg på.

7.4 Begjæring om sletting

Som nevnt under kapittel 6 skal virksomhetene slette personopplysninger når formålet med den enkelte behandling er oppnådd, med mindre det kan dokumenteres fastsatt oppbevaringsrett eller -plikt i medhold av lov eller forskrifter.[46] Virksomheten må derfor etablere og dokumentere systematiske sletterutiner og sikre etterlevelse av disse. I tillegg kan den som er registrert i visse tilfeller begjære sletting.[47]

Eksempler der sletting er aktuelt etter begjæring fra kunden:

- der den enkelte trekker tilbake samtykket som ligger til grunn for behandlingen og det ikke foreligger annet behandlingsgrunnlag,[48]
- der den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 1 og virksomheten ikke kan påvise tungtveiende berettigede grunner til behandlingen, eller den registrerte protesterer i henhold til artikkel 21 nr. 2,[49]
- der det pågår en ulovlig behandling,[50]

7.5 Portabilitet

Retten til dataportabilitet etter personvernforordningen innebærer en rett til å overføre personopplysningene sine fra en virksomhet til en annen eller til å få disse utlevert i et strukturert, alminnelig anvendt og maskinlesbart format.[51]

[45] *Personvernforordningen artikkel 16*
[46] *Se personvernforordningen artikkel 5 pkt. 1 bokstav e).*
[47] *Se personvernforordningen artikkel 17 om "Retten til å bli glemt"*
[48] *Se personvernforordningen artikkel 17 nr. 1 bokstav b jfr artikkel 6 og 9*
[49] *Se personvernforordningen artikkel 17 nr. 1 bokstav c*
[50] *Se personvernforordningen artikkel 17 nr. 1 bokstav d*
[51] *Se personvernforordningen artikkel 20*

Personopplysningene som den enkelte ønsker utlevert må være gitt til virksomheten på bakgrunn av samtykke eller avtale. Dette innebærer at innsamling som følger av lov eller forskrift faller utenfor bestemmelsen om dataportabilitet i personvernforordningen, samtidig som slike bestemmelser i seg selv kan gi en tilsvarende rett til overføring av slike opplysninger. Dette er tilfellet for energibransjen som har hatt løsninger for slik tilgjengeliggjøring lenge før ny personvernforordning trådte i kraft. Se bl.a. regulering av tilgang til historiske forbruksdata i avregningsforskriften. Det betyr at historiske data kan tilgjengeliggjøres, for eksempel til energirådgivere.[52] Dette innebærer at det gjøres en eksport av/tilgang til opplysningene for hver begjæring. Tilgang til måleverdier for tredjeparter i et aktivt kundeforhold gjøres gjennom tredjepartstilgang via elhub, alternativt om det er ønskelig med løpende tilgang til data, fra HAN-port.

Rettigheten etter personvernforordningen gjelder videre kun opplysninger som den registrerte har gitt den behandlingsansvarlige. Dette omfatter også opplysninger som er samlet inn fra den enkelte gjennom vedkommendes aktive bruk av en tjeneste, for eksempel gjennom strømforbruk. Opplysninger som er samlet inn fra andre enn den registrerte, faller imidlertid utenfor. Rettigheten gjelder ikke data som er bearbeidet av virksomheten, slik som for eksempel analyser og utarbeidelse av profiler. Tekniske data knyttet til det elektriske anlegget i huset/leiligheten, anses heller ikke omfattet av rett til overføring. Dette er informasjon som er knyttet til anlegget og ikke den som til enhver tid er kunde.

I tillegg, hvis det er teknisk mulig, kan den registrerte kreve at virksomheten sørger for å overføre opplysningene direkte til den nye virksomheten.

Når en person utøver retten til dataportabilitet etter personvernforordningen, mister man ikke de andre rettighetene man har i henhold til personopplysningsloven, og opplysningene skal fortsatt behandles hos den behandlingsansvarlige virksomheten.

- Personopplysningene som er gitt til virksomheten på bakgrunn av samtykke eller avtale kan kreves portert. Informasjonen skal i slike tilfeller leveres i et strukturert, alminnelig anvendt og maskinleselig format.
- Personen som fremmer krav om dataportabilitet må kunne identifiseres som den registrerte, før tilgjengeliggjøring av aktuell opplysninger kan finne sted.[53]

7.6 De øvrige rettighetene (reservasjon mv)

I tillegg til rettigheter som fremkommer av punkt 7.1 – 7.5 over, har personvernforordningen bestemmelser om rett til begrensning av behandling,[54] rett til å protestere og regulering av automatiserte individuelle avgjørelser, herunder profilering.[55]

Det er så langt ikke blitt identifisert forhold som har foranlediget særskilte merknader til disse rettighetene. Disse rettighetene er derfor ikke nærmere behandlet i denne versjonen av dokumentet.

[52] Se også avregningsforskriften § 8-1, 5. ledd og § 8-2
[53] Se omtale av identifisering i forbindelse med innsyn i punkt 8.2
[54] Se personvernforordningen artikkel 18
[55] Se personvernforordningen artikkel 22

8. Personvernkonsekvenser og risikoanalyse

Virksomhetene skal både gjennomføre vurderinger av personvernkonsekvenser (DPIA[56]) når det er påkrevd og alltid gjøre risiko- og sårbarhetsvurderinger (ROS) for å sikre et egnet sikkerhetsnivå.[57] Begge vurderinger innebærer en analyse av sannsynligheten for og konsekvensene av uønskede hendelser. Formålet med vurderingene er å kunne identifisere og implementere tiltak for å forebygge eller redusere de uønskede hendelsene. I tillegg, skal slike vurderinger legge til rette for ivaretakelse av krav til innebygd personvern.[58]

8.1 Vurdering av personvernkonsekvenser (DPIA)

En vurdering av personvernkonsekvenser[59] skal sikre at rettighetene og frihetene til de som er registrert i behandlingen ivaretas. Ved gjennomføringen skal virksomheten alltid rådføre seg med personvernombudet om virksomheten har etablert dette. I tillegg skal det vurderes å innhente synspunkter fra representanter fra de registrerte.[60]

8.1.1 Når skal man gjennomføre en vurdering av personvernkonsekvenser?

Virksomhetene skal gjennomføre vurdering av personvernkonsekvenser når det er trolig at en type behandling vil medføre høy risiko for de registrertes rettigheter og friheter. Hensikten er å sikre at krav til personvern samt interessene til de registrerte er tilstrekkelig ivaretatt. Vurderingen skal skje når virksomheten tar i bruk nye produkter, tjenester eller systemer, og særlig ved bruk av ny teknologi på innovative måter.

Det skal gjøres en vurdering av personvernkonsekvenser dersom to eller flere av følgende kriterier er oppfylt:

- Personopplysninger behandles i stor skala (stort antall kunder i forhold til egen totale kundeportefølje)
- Beslutninger med betydelig virkning for kundene gjøres ved automatiske avgjørelser
- Systematisk monitorering av individer for å sammenligne kundedata mellom individer og grupper
- Sammenstilling av flere datasett
- Innovativ bruk av ny teknologi
- Endringer som påvirker kundenes tilgang til en tjeneste eller mulighet for å inngå en avtale

[56] *Se personvernforordningen artikkel 35*
[57] *Se personvernforordningen artikkel 24, 25, 32 og 35 der det stilles det krav til at behandlingsansvarlig og databehandler skal gjøre risikovurderinger.*
[58] *Se personvernforordningen artikkel 25 om innebygd personvern og personvern som standardinnstilling.*
[59] *Se personvernforordningen artikkel 35*
[60] *Se personvernforordningen artikkel 35 pkt. 9.*

Det skal gjøres en vurdering av personvernkonsekvenser dersom to eller flere av følgende kriterier er oppfylt (forts.):

- Profilere, evaluere eller rangere kundene på bakgrunn av nettanalyser, forbruksmønster mv.
- Bruk av særlige kategorier av personopplysninger eller opplysninger av svært personlig karakter
- Bruk av personopplysninger om sårbare registrerte

Eksempler	Anbefales det å gjennomføre en DPIA?	Kriterier som anses oppfylt
Virksomheten ønsker å gjennomføre analyse på kundeopplysninger på tvers av formål (navn, bosted, alder, strømforbruk, opplysninger fra avtale mv) for å forbedre egne prosesser samt vurdere om det er marked for nye tjenester.	Ja	• Personopplysninger behandles i stor skala • Sammenstilling av datasett
Virksomheten sender generiske nyhetsbrev og tilbud til kundene sine basert på samtykke.	Nei	• Personopplysninger behandles i stor skala
Virksomheten oppdaterer løsningen ved å bytte system.	Nei	• Personopplysninger behandles i stor skala
Virksomheten ønsker å gjøre endringer på formatet på faktureringsskjema. Innholdet for øvrig endres ikke.	Nei	• Personopplysninger behandles i stor skala
Gi kunde mulighet til personlig tilpassende tilbud og markedsføring basert på profilering.	Ja	• Sammenstilling av datasett • Automatiske beslutninger
Analysere forskjell på strømforbruk til kunden over tid basert på kartlegging av variasjon i strømforbruk.	Ja	• Systematisk monitorering av individer • Innovativ bruk av ny teknologi
Lage en «min side» løsning for kundene ved å tilgjengeliggjøre blant annet kontaktopplysninger og historikk på fakturaer mv.	Nei	• Personopplysninger behandles i stor skala • Bruk av ny teknologi
Bruk av kunstig intelligens for å skaffe tilstrekkelig innsikt for å automatisere kundedialogen.	Ja	• Personopplysninger behandles i stor skala • Bruk av ny innovativ teknologi
Endre «min side» løsning på nettside ved å inkludere et diagram som synliggjør hva kunde betaler for per måned mellom nettleie og strøm (i tillegg til faktura)	Nei	▪ Personopplysninger behandles i stor skal

8.1.2 Gjennomføring av personvernkonsekvensvurdering

Virksomheten skal gjennomføre en vurdering av risikoen for konsekvenser for den registrertes rettigheter og friheter, samt beskrive tiltak for å redusere risikoene. Risikoen for personvernet vurderes ved bruk av sannsynlighet og konsekvens:

- Sannsynlighet er muligheten for at risikoen skal inntreffe.
- Konsekvens for den registrertes rettigheter og friheter og hvor alvorlig denne er.

Konsekvensen av at rettighetene og frihetene ikke blir innfridd kan være både være fysisk, materiell og ikke-materiell skade. Konsekvensene behandlingen har for de registrerte er ikke avhengig av at det skjer en hendelse, men kan også inntreffe gjennom selve behandlingen i seg selv.

For å vurdere personvernkonsekvenser, tas det utgangspunkt i personvernprinsippene og hvordan disse er ivaretatt for å sikre de registrertes rettigheter og friheter. Personvernprinsippene vurderes i personvernkonsekvensvurderingen ved å ta utgangspunkt i ulike scenario og se på risikoer knyttet til hvert enkelt av disse.

Vedlagt følger en liste over forslag til eller eksempler på en rekke personvernscenarioer det kan tas utgangspunkt i. Det må vurderes konkret hvorvidt disse er relevante, og hvilke andre scenarioer som eventuelt er relevant å ta i betraktning. Det vil både være hensiktsmessig og nødvendig å tilpasse scenarioene etter behov, slik at det treffer prosjektet/endringen/området på best mulig måte.

8.2 Risiko- og sårbarhetsvurdering (ROS)

Virksomhetene skal alltid gjennomføre Risiko- og sårbarhetsvurdering[61] ved endringer som kan påvirke informasjonssikkerheten. Endringer kan være knyttet til endringer i behandlinger, i systemer, leverandører eller organisering eller endringer i trusselbildet. I tillegg bør en slik vurdering gjøres minst årlig for å fange opp endringer i virksomheten eller endrede vurdering av trusselbildet.

Risikovurderinger skal omfatte en vurdering av sannsynlighet og konsekvens av uønskede hendelser som påvirker ivaretakelse av informasjonssikkerheten, både for virksomheten og for den som blir registrert. Vurderingene og aktuelle tiltak skal ta hensyn til behandlingens art, omfang, formål og konteksten.[62]

Det er dermed flere og andre aspekter enn konsekvenser for den registrerte som skal vurderes i en risikovurdering i motsetning til DPIA. Det er likevel mulig og ofte ønskelig å gjennomføre både risikovurderingen og DPIA sammen. Disse kan gjennomføres ved hjelp av samme mal så lenge det er en tydelig skille mellom hvilken risiko er knyttet til virksomhetens risiko og hvilke risikoer det er for personopplysningssikkerheten til den registrerte. Det kan imidlertid være hensiktsmessig å diskutere med andre ressurser i forbindelse med en ROS enn ved en DPIA. Se vedlegg 3 for et eksempel på mulig skala for hhv sannsynlighet og konsekvenser.

[61] Personvernforordningen artikkel 24, 25, 32 og 35 stiller krav til at behandlingsansvarlig og databehandler skal gjøre risikovurderinger
[62] Se personvernforordningen artikkel 32

9. Informasjonssikkerhet

I henhold til personopplysningsloven handler informasjonssikkerhet[63] om å sikre personopplysningenes konfidensialitet, tilgjengelighet og integritet. Dette er krav som krever tiltak som overlapper med krav fra andre lover og forskrifter som treffer bransjen. Det er viktig å merke seg at for denne bransjen er alle aspektene sentrale, slik at både konfidensialitet for personopplysninger, ivaretakelse av integritet slik at det er korrekte opplysninger som danner grunnlag for korrekte avregningsdata og leveranser samt sikre høye krav til tilgjengelighet for nett- og strømleveranser, er alle sentrale aspekter som må ivaretas.

Krav til grunnsikring i beredskapsforskriften og andre lover og forskrifter med tilsvarende krav[64] gjelder også ved behandling av personopplysninger. Ved å følge slike krav, vil man normalt også oppnå et tilstrekkelig sikkerhetsnivå for personopplysninger.

Konfidensialitet	Sikre at opplysningene behandles i samsvar med taushetsplikt og andre hensyn slik at informasjon ikke blir gjort tilgjengelig for uvedkommende.
Tilgjengelighet	Sikre at personopplysninger er tilgjengelige for rettmessige brukere når de har behov for det.
Integritet	Sikre opplysningene mot at det utføres uautorisert eller utilsiktet endring uten at dette avdekkes

Virksomheten må foreta en klassifisering av aktuelle personopplysninger ut fra behov for konfidensialitet, integritet og tilgjengelighet. I vedlegg 2 er det gitt eksempler på tabell over mulig klassifisering som fastsetter nivåer i forskjellige konfidensialitets-, integritet- og tilgjengelighetsklasser.

Sikkerhetsmål og vurderinger av akseptabelt sikkerhetsnivå skal defineres i styrende dokumenter i virksomhetens internkontrollsystem.

Behovet for hensiktsmessige sikkerhetstiltak identifiseres gjennom risikoanalyser slik som omtalt i kapittel 8. Tiltak kan være enten organisatoriske, tekniske eller fysiske.

[63] *Personvernforordningens artikkel 32 om sikkerhet ved behandlingen*
[64] *Se oversikt over sentrale lover på Energi Norges hjemmeside*

Eksempler på tiltak:

- Låser på dører og porter
- Inngangskontroll
- Krav til dokumentsikkerhet
- Tilgangsstyring til applikasjoner
- Kryptering av elektronisk kommunikasjon
- Opplæringstiltak innen sikkerhetskultur for egne ansatte

Den enkelte virksomhet må vurdere om det foreligger særskilte forhold eller typer personopplysninger og behandlinger som tilsier behov for iverksettelse av ytterligere sikringstiltak. Dette kan for eksempel være behov for ytterligere tiltak når virksomheten behandler personopplysninger om personer med adressesperre av type kode 6 eller 7.

Krav til behandling av personopplysninger om personer med adressesperre av type kode 6 eller 7:

- Adressesperre er såkalte graderte adresser og er tidligere blitt omtalt som kode 7 og kode 6. Strengt fortrolig adresse er den strengeste adressegraderingen (Kode 6). Beslutningsmyndighet om adressesperre er delt mellom Kripos og Skattedirektoratet (Barnevernssaker). Begrepene kommer fra Beskyttelsesinstruksen. Det er Folkeregisterloven § 10-4 som regulerer tilgang til opplysninger gradert i medhold av beskyttelsesinstruksen. Virksomheten må innenfor sitt selvstendige behandlingsansvar vurdere kundehåndtering av personer med høyt beskyttelsesbehov.
- Det er fastsatt egne retningslinjer i bransjen som er tilgjengelig for ansatte med roller som tilsier at vedkommende har tjenstlig behov for tilgang til denne retningslinjen og til rutinebeskrivelsene. Disse skal følges og den enkelte virksomhet skal ikke etablere egne rutiner som avviker fra dette.
- Også kunder med adressesperre kode 6 eller 7 skal håndteres med utgangspunkt i Avregningsforskriften.

Det skal ikke i fritekstfelter eller på annen måte direkte eller indirekte føres notater som kan indikere adressesperre eller lignende beskyttelsesnivå, ettersom f.eks. fritekstfelt for anleggsbeskrivelse utveksles mellom markedsaktørene via Elhub.

- Det kan være hensiktsmessig som et forebyggende tiltak å redusere omfang av bruk av fritekstfelter, da det eller er lett at de benyttes til opplysninger som kan indikere en husholdningskundes helsetilstand eller andre opplysninger som anses som særlig kategori personopplysninger. Dette gjelder i alle tilfeller opplysningene kan knyttes til identifiserbar enkeltperson enten det er eier eller bruker av anlegg.
- Om fritekstfelt benyttes på en slik måte, stiller det strengere krav til tilgangsstyring og andre tiltak enn det som ellers ville vært nødvendig.

9.1 Særlig om krav til tilgangsstyring

Tilgangsstyring handler om å ha kontroll med hvem som har adgang til hvilken informasjon og hvilke systemer. Det er en viktig del av virksomhetenes sikring av personopplysninger.

9.1.1 Tjenstlig behov

Tilganger skal tildeles og benyttes i tråd med tjenstlig behov. Kravene gjelder både behandling av opplysninger som lagres elektronisk og som lagres fysisk på papir. Hva som anses som hensiktsmessige og tilstrekkelige tiltak, vil naturlig nok være av forskjellige karakter avhengig av oppbevaringsmåte. Virksomheten skal for alle systemer kunne dokumentere hvem som har hvilke tilganger og hvem som har benyttet tilganger til å gjøre oppslag i noens personopplysninger. Det tjenstlige behovet for tilgang til de ulike systemene og dataene, skal være dokumentert. Om ikke alle systemer har tilfredsstillende tilgangsstyring, er det viktig at dette er dokumentert, ledelsen informert og at det foreligger en plan for utbedring eller utfasing.

Virksomheten må også kunne dokumentere at tilstrekkelig opplæring er gitt og at taushetserklæring er signert før tilganger gis.

Eksempler på tjenstlig behov:

Montør:
Montører har oppgaver hvor de kan få tilgang til personopplysninger, eksempelvis ved spennings- og målerkontroller. De aktuelle systemene må legge til rette for at disse ikke har tilgang til personopplysninger ut over det som trengs for å utføre det enkelte oppdrag. Selv om oppgaven eksempelvis er frakopling på grunn av manglende betaling, trenger ikke montøren tilgang til reskontrosystemet og andre sensitive personopplysninger for å utføre sine oppgaver og skal derfor heller ikke ha slik tilgang. Slike oppdrag skal fortrinnsvis løses ved hjelp av tilpassede arbeidsordrer, som eventuelt kan kvitteres ut elektronisk.

Entreprenører mv:
Øvrige eksterne aktører, f.eks. ansatte i andre virksomheter i konsernet, entreprenører eller sakkyndige virksomheter, skal på samme måte ikke tildeles direkte adgang til personopplysninger i systemene, men fortrinnsvis utføre arbeidet basert på tildelte arbeidsordrer inneholdende navn, adresse, telefonnummer og enkelte tekniske data som er nødvendig for å utføre det aktuelle oppdraget.

9.1.2 Behov for begrenset tilgang

Virksomhetene må vurdere hvor mange, og hvilke personer eller roller som skal kunne håndtere personopplysninger av mer sensitiv karakter. Eksempelvis kunder med helseerklæring eller betalingsvansker. Det kan være hensiktsmessig å begrense antall ansatte som har tilgang til slike kategorier av data. Dette vil også kunne redusere behovet for oppfølging og kontroll.

9.1.3 Jevnlig kontroll

Virksomheten skal påse og jevnlig kontrollere at personell med adgang til personopplysninger er autorisert for tilgang til slike opplysninger. Det er virksomheten selv som vurderer og autoriserer de som skal ha tilgang til personopplysninger basert på tjenstlig behov. Virksomheten plikter å jevnlig kontrollere hvorvidt behov for tilgang fortsatt er til stede, og fastsette frekvens for gjennomgang av autorisasjoner. Rutiner i denne forbindelse skal være dokumentert.

Ansattes oppslag i personopplysninger skal loggføres og oppbevares på elektronisk medium i minst 3 måneder. Virksomheten skal gjennom stikkprøver eller annen type kontroll, undersøke om ansatte benytter tilganger til andre formål utover tjenstlig behov. Slike kontrollrutiner skal være dokumentert. Resultatet skal dokumenteres.

Om tiltak knyttet til tilgangsstyring ikke implementeres, må vurderingene dokumenteres og være godkjent av leder med tilstrekkelig fullmakt til å akseptere en slik risiko.

9.2 Krav til sikring av kommunikasjon og overføring av personopplysninger

Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.

Forsendelse av fødselsnummer og taushetsbelagt informasjon vil typisk kreve sikring i form av kryptering ved bruk av e-post. Virksomheter skal kreve minimum to-faktor autentisering ved tilgang til informasjon på en portal.

Det er viktig å notere at krav som stilles til sikring av kommunikasjon og overføring av personopplysninger vil kun variere over tid. En virksomhet må derfor kontinuerlig revurdere tidligere beslutninger og følge med utviklingen av hva som anses som tilfredsstillende sikker kommunikasjon for ulike typer personopplysninger.

9.3 Logging, loggoppfølging, overvåking

Virksomheten må logge alt som har betydning for informasjonssikkerheten, herunder aktivitet på systemer, programmer, filer, internett og skrivere. Arbeidsgiver kan benytte loggene til overordnet systemovervåking eller generell kontroll av datasystemet. Slik kontroll kan kun aggregeres på gruppenivå eller for deler av virksomheten. De kan ikke benyttes som kontrolltiltak overfor enkelte ansatte, uten at slikt tiltak er i tråd med arbeidsmiljølovens bestemmelser for slike kontroller.[65]

[65] *Kontrolltiltak rettet mot ansatte må både oppfylle krav til personvern og arbeidsmiljølovens kapittel 9.*

10. Personopplysninger i utviklings- og testmiljø

I tidlige utviklings- og testfaser skal det benyttes fiktive eller anonymiserte data. Det kan i noen situasjoner være nødvendig å benytte reelle personopplysninger. Dette vil for eksempel kunne gjelde i den avsluttende testperioden før overgang til produksjonssetting. I tillegg kan det være behov for å benytte reelle personopplysninger for testing av informasjonsflyt på tvers av aktører, for eksempel ved endringer i overføring til Elhub. Det vil ofte være berettiget interesse som utgjør behandlingsgrunnlaget for en slik bruk av personopplysninger.

Ved bruk av personopplysninger i forbindelse med gjennomføring av tester, må virksomheten påse på at:

- det bare skjer der det er umulig eller uforholdsmessig vanskelig å benytte anonyme eller fiktive opplysninger som gir tilstrekkelig kvalitet
- krav til dataminimering og lagringsbegrensning er ivaretatt
- testingen gjennomføres på en så lite inngripende måte som nødvendig
- vurderinger knyttet til slik bruk er dokumentert
- de berørte er informert om at deres personopplysninger brukes som testdata
- testdatasett ikke oppbevares lengre enn det som er nødvendig for formålet.
- testdatabaser og testdatasett basert på reelle data håndteres med de samme sikkerhetskrav som den "skarpe" databasen.

11. Utleveringer

Det skal foreligge behandlingsgrunnlag for utlevering[66] av personopplysninger til en tredjepart. Den registrerte skal informeres om utleveringen og hvem opplysningene utleveres til, med mindre det foreligger eksplisitte hjemler for å unnta slik informasjon, se kapittel 7.

Alle utleveringer skal dokumenteres. Hver utlevering skal i ettertid kunne kobles til den registrerte det er utlevert informasjon om.

Eksempler på utleveringer:

- Den registrerte samtykker i utleveringen. Virksomheten kan for eksempel innhente samtykke til å utlevere opplysninger til en ekstern tredjepart. Dette kan for eksempel være en energirådgiver.
- Utlevering av personopplysninger basert på avtale med kunde:
- Innhenting av kredittvurderinger.
- Utveksling av personopplysninger mellom nettselskapet og strømleverandør.
- Oversendelse av klagesak til Elklagenemnda.
- Utleveringen er fastsatt i lov. Eksterne aktører må vise til hvilket rettslig grunnlag de ber om tilgang til personopplysninger etter, for å kunne få tilgang til personopplysninger om kunder og andre. Noen praktiske eksempler:
    - Politiet: Virksomhetene plikter å utlevere personopplysninger som kan antas å ha betydning i en pågående sak, jf. straffeprosessloven § 210 første ledd. Dersom det er fare for at etterforskningen vil lide i påvente av rettens kjennelse, kan politiet også henvende seg til påtalemyndigheten for en ordre om utlevering av opplysninger, jf. straffeprosessloven § 210 annet ledd.
    - Retten: Virksomhetene plikter å forklare seg for retten etter straffeprosessloven § 237 (1).
    - Inkasso: Det følger forutsetningsvis av inkassoloven § 2 at inkassatorer har adgang til å samle inn personopplysninger for gjeldsinndrivelse. Tilsvarende har virksomhetene rett til å utlevere personopplysninger i forbindelse med inkassovirksomhet.

[66] *Personvernforordningen artikkel 4, pkt. 2) angir "utlevering ved overføring" som eksempel på en behandling av personopplysninger. Tilsvarende som for andre behandlinger må det foreligge et behandlingsgrunnlag. Se artikkel 6 pkt. 1 for behandlingsgrunnlag.*

12. Databehandleravtaler

En behandlingsansvarlig virksomhet må påse at det inngås tilstrekkelige avtaler der en tredjepart behandler personopplysninger på vegne av virksomheten.[67] Dette kan typisk være en driftsleverandør som drifter et eller flere IT-systemer og i den forbindelse har adgang til personopplysninger om ansatte eller kunder.

12.1 Krav til vurderinger før databehandler velges

Ansvaret gir seg bl.a. uttrykk i innføring av et uttrykkelig krav til den behandlingsansvarliges vurdering av databehandlers egnethet, før valget av databehandler gjøres. Det kan bare brukes databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene. Dette stiller krav til selve utvelgelsesprosessen i forkant av selve avtaleinngåelsen, i tillegg til krav til selve avtaleinnholdet og presisjonen her.

Virksomheten bør evaluere leverandørens dybdekunnskap, pålitelighet og tilgang til ressurser før denne velges som databehandler. Overholdelse av godkjente adferdsnormer samt bruk av sertifiseringsmekanismer kan tjene som garanti. For å vise ansvarlighet anbefales det at virksomheten dokumenterer vurderingen som er gjort av databehandleren før avtale inngås.

12.2 Krav til databehandleravtaler

En databehandler skal behandle personopplysninger i samsvar med de rutiner som den behandlingsansvarlige har oppstilt og kan ikke behandle personopplysninger på annen måte, eller for andre formål enn det som følger av den skriftlige avtalen. Det er derfor viktig at det foreligger klare og tydelige avtaler.

Avtalen skal inneholde en beskrivelse av behandlingen i tillegg til å pålegge databehandleren aktuelle plikter i tråd med kravene til slike avtaler.[68]

Det er videre viktig å sikre kontroll over verdikjedene. Det er eksplisitt uttrykt at en databehandler ikke kan engasjere en underleverandør som får tilgang til personopplysninger uten tillatelse fra den behandlingsansvarlige.[69] Selv om dette er et lovkrav, anbefales at dette også reguleres eksplisitt i avtalen, og at det i tillegg sies noe om prosessen og fremgangsmåte ved et ønske om å benytte eller skifte foreliggende underdatabehandler mv.

[67] *Personvernforordningen artikkel 28 regulerer databehandlere, herunder databehandleravtaler i pkt. 3*
[68] *Se personvernforordningen artikkel 28 (3)*
[69] *Se personvernforordningen artikkel 28 pkt. 2)*

12.3 Oppfølging av avtalen

Virksomheten må etablere rutiner som sikrer oppfølging av at leverandøren gjennomfører behandlingen i samsvar med avtalen i avtaleperioden.

- En databehandleravtale skal gi konkrete rammer for de aktuelle behandlingene en databehandler skal gjøre på vegne av den behandlingsansvarlige. Det krever tilsvarende presise beskrivelser i databehandleravtalen.
- Hva som er tilstrekkelig, er avhengig av hva bl.a. hvilken type behandling tredjepart gjør på vegne av virksomheten. Det vil også kunne ha betydning hvilken relasjon de har til hverandre. Om det er andre selskap i et konsern som utfører oppgaver for et annet selskap, kan det være tilstrekkelig med enklere avtale enn om det er en ekstern aktør. Dette fordi selskaper et konsern ofte har samme interne rammeverk, policyer, retningslinjer som ivaretar krav til personvern og informasjonssikkerhet på en ensartet måte.
- I Vedlegg 5 er det utarbeidet en sjekkliste for oppfølging av databehandlere – der kravene til innhold i avtaler er omsatt til kontrollspørsmål. Den behandlingsansvarlige kan da benytte disse som underlag for å vurdere hva som må beskrives og stilles krav om i den enkelte avtale, slik at alle krav i tilstrekkelig grad er ivaretatt.

13. Brudd på personopplysnings-sikkerheten

Brudd på personopplysningssikkerheten[70] er definert som brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

En virksomhet som opplever brudd på personopplysningssikkerheten som følge av avvik i interne rutiner eller datasikkerheten, må kunne[71]:

- Identifisere avvik
- Utrede og løse avvikene
- Begrense skadene for de(n) registrerte
- Varsle Datatilsynet og de(n) registrerte når avvikets type og omfang tilsier det
- Dokumentere alle avvik uavhengig av om disse er meldepliktige til Datatilsynet
- Være i stand til å lære av de avvikene som oppstår for å hindre gjentakelse.

Slike prosesser kan være tidskrevende i en situasjon hvor tid mangler, det er dermed viktig å ha gode rutiner og et etablert samarbeid med kontaktpunkt på tvers av verdikjeden i forkant.

13.1 Alle uønskede hendelser og avvik skal registreres internt

Alle uønskede hendelser bør dokumenteres internt i virksomheten uavhengig av om dette er avvik som er meldepliktige til Datatilsynet. Dette vil kunne bidra til økt bevissthet knyttet til hva som er uønskede hendelser og avvik, samt sikre læring og kontinuerlig forbedring også av mindre alvorlige hendelser. På denne måten vil også brudd på andre bestemmelser i personopplysningsloven enn det som omfatter personopplysningssikkerhet, kunne fanges opp på en systematisk måte.

Slik registrering bør bl.a. omfatte informasjon om de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det.

13.2 Varsel til Datatilsynet

Virksomheten skal i utgangspunktet melde alle avvik som innebærer brudd på personopplysningssikkerheten til Datatilsynet.[72] Unntak kan gjøres når det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter, noe som omfatter både personvernrettigheter og andre grunnleggende rettigheter.[73]

[70] *Se personvernforordningen artikkel 33 og 34*
[71] *Se personvernforordningen artikkel 33 og 34*
[72] *Se personvernforordningen artikkel 33*
[73] *Se personvernforordningen artikkel 4 nr. 12*

Hvorvidt det er behov for å melde fra til Datatilsynet eller de berørte beror på en konkret vurdering av avviket, omstendighetene rundt avviket, alvorlighetsgrad og risiko for de berørte:

- Ved ingen eller lav risiko, skal verken Datatilsynet eller de registrerte varsles.
- Ved middels risiko må Datatilsynet varsles, men ikke de berørte.
- Ved høy risiko skal både Datatilsynet og de berørte varsles.

Varsling til Datatilsynet skal skje innen 72 timer etter at man har fått kjennskap til bruddet. Dersom virksomheten ikke har fullstendig oversikt over avviket kan det meldes inn trinnvis. Om det meldes senere enn 72 timer, må årsaken til forsinkelsen oppgis.

Det er den behandlingsansvarlig som har plikt til å melde til Datatilsynet. Varsling fra behandlingsansvarlig bør med fordel vise frem hvilke andre parter i verdikjeden som er involvert i avviket. Det samme gjelder der flere behandlingsansvarlige hver for seg melder om brudd i samme verdikjede.

Varslet skal som minimum inneholde:

- En beskrivelse av avviket, hva slags personer og personopplysninger som er berørt.
- Et anslag på hvor mange personer og oppføringer av personopplysninger som er berørt av sikkerhetsbruddet.
- En beskrivelse av hvilke konsekvenser avviket trolig vil ha.
- En beskrivelse av de tiltak som er planlagt iverksatt for å lukke avviket og begrense konsekvensene av det.
- Inneholde navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes.

Det er utarbeidet et skjema i Altinn for melding av avvik. Dette skal som hovedregel benyttes. Det viktigste er imidlertid å varsle. Om det er forhold som forhindrer å varsle raskt via Altinn, kan også varsel gis på andre måter.

13.3 Varsel til den berørte

Den registrerte[74] skal varsles dersom det er sannsynlig at avviket vil medføre en høy risiko for de berørte personene. Den som er berørt skal varsles slik at vedkommende settes i stand til å ivareta egne interesser. Det skal varsles uten unødig opphold.

Eksempler på meldeplikt - når bruddet kan føre til:

- ID tyveri
- Økonomisk tap
- Tap av omdømme
- Bedrageri eller svindel

Hvordan varsel gis, må vurderes konkret ut fra den aktuelle situasjonen, hastegrad, hvordan kommunikasjonen normalt er med den registrerte og hva avviket består i.

[74] *Se personvernforordningen artikkel 34*

Varsel til den registrerte skal inneholde:

- Beskrivelse av avviket
- Beskrive sannsynlige konsekvenser av avviket
- Beskrivelse av tiltak som er utført/i ferd med å utføres.
- Anbefalinger om tiltak som den enkelte selv kan eller bør iverksette for å begrense skade/uønskede konsekvenser
- Kontaktinformasjon om spørsmål, herunder kontaktinformasjon til eventuelt personvernombud i virksomheten.

Virksomheten kan la være å varsle til den registrerte på visse vilkår:[75]

- Dersom det er iverksatt beskyttelsestiltak for personopplysningen som er omfattet av sikkerhetsbruddet, særlig dersom tiltakene gjør opplysningene uleselige for uvedkommende. Typisk gjennom tilstrekkelig kryptering.
- Dersom det er iverksatt etterfølgende tiltak som gjør at risikoen sannsynligvis ikke lenger er reell.
- Hvis det er uforholdsmessig vanskelig å varsle hver enkelt av de berørte. I slike tilfeller skal informasjonen offentliggjøres eller deles på annen måte, slik at de berørte likevel underrettes på en effektiv måte.

Risikoen ved et avvik kan fastsettes ved en vurdering av følgende kriterier:

- Type brudd: Brudd på konfidensialitet, tilgjengelighet, integritet eller en kombinasjon av disse
- Personopplysningenes art, sensitivitet og mengde
- Hvor lett det er å identifisere enkeltpersoner:
  - Mulighet for sammenstilling med annen data for å oppnå identifisering
  - Vurdering av hvor sikker kryptering og oppbevaring av tilgangsnøkkel er
- Konsekvenser for den berørte:
  - Alvorlighetsgrad av konsekvenser, eks. psykisk og fysisk skade, ydmykelse, svindel, ID-tyveri
  - Om det er langvarige eller kortvarige konsekvenser
- Spesielle egenskaper ved berørte enkeltpersoner:
  - Bruddet omfatter barn eller sårbare enkeltpersoner eller utsatte grupper der konsekvensene kan bli mer omfattende eller alvorlig enn normalt
- Antall berørte enkeltpersoner
- Type behandling og personopplysninger

[75] *Se personvernforordningen artikkel 34 nr. 3*

Eksempler på avvik og om disse som hovedregel medfører meldeplikt

Det understrekes at dette bare er et utgangspunkt og at det alltid må foretas en konkret vurdering av risikoen og at denne vurderingen må dokumenteres.

Hendelser	Skal som hovedregel meldes til Datatilsynet?	Skal som hovedregel meldes til den berørte?
Tyveri av bærbart utstyr som inneholder personopplysninger og innholdet ikke er kryptert	Ja	Ja
Forsendelse av særlige kategorier av personopplysninger usikret i e-post til alle kunder	Ja	Ja
Utleveringer av personopplysninger uten rettslig grunnlag til for eksempel inkasso	Ja	Ja
Forsendelse av særlige kategorier personopplysninger til feil mottaker per post eller e-post	Ja	Ja
Forsendelse av personopplysninger uten særlige kategorier av personopplysninger til feil mottaker	Nei	Ja
Forsendelse ril riktig mottaker per post eller e-post, som ved en feil inneholder særlige kategorier personopplysninger om andre	Ja	Ja
Oppdaget mangelfull sletting av informasjon på et sikre interne system som inneholdt kun kontaktopplysninger til alle kundene	Ja	Nei
Datainnbrudd på et system som inneholder personopplysninger til kundene	Ja	Ja
Fysisk innbrudd hvor ukryptert data eller papirdokumenter som inneholder personopplysninger er forsvunnet	Ja	Må vurderes
Kasting av papirdokumenter som inneholder personopplysninger uten makulering	Ja	Må vurderes
Avhending av utstyr uten forsvarlig sletting av personopplysninger	Ja	Må vurderes
Publisering av personopplysninger på nettet som ikke skulle ha vært publisert, eller at personopplysningene ikke har blitt anonymisert	Ja	Må vurderes
Samtykkeerklæringer som ikke er tilstrekkelig informerte og dermed ugyldige	Ja	Ja
Manglende tilgangsstyring eller feil ved denne som fører til at uvedkommende har fått tilgang til særlige kategorier personopplysninger	Ja	Ja
Manglende tilgangskontroll som gjøre at flere ansatte fikk tilgang til personopplysninger uten tjenstlig behov	Nei	Nei

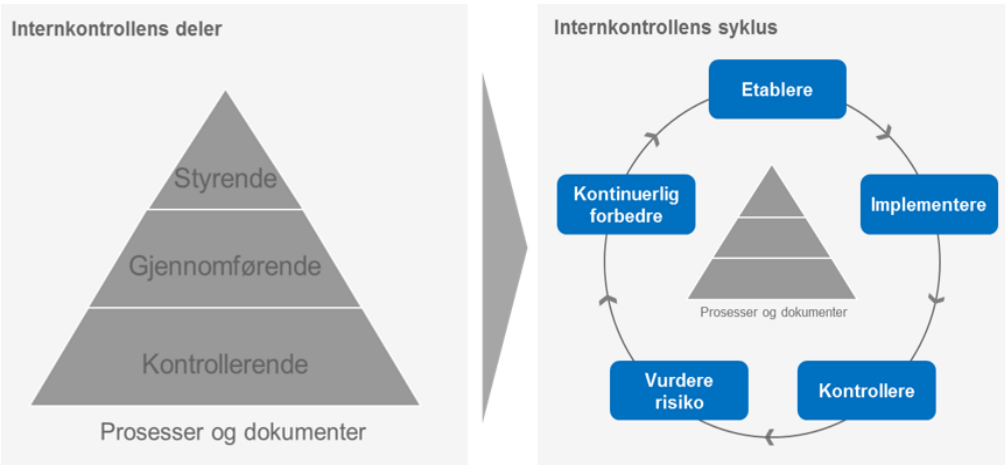
14. Internkontroll

For å kunne identifisere og ta i bruk egnede tekniske og organisatoriske tiltak, er det behov for en systematisk tilnærming. Tiltakene skal ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad. Det er videre et krav om å både sikre og dokumentere at behandlingen av personopplysninger skjer i samsvar med kravene i personopplysningsloven, også over tid. Dette krever en hensiktsmessig internkontroll.

Internkontroll må ses på som en prosess og skal være et praktisk verktøy for å sikre at opplysninger blir behandlet på en lovlig, sikker og forsvarlig måte. Dette innebærer både prosesser for å styre, gjennomføre samt kontrollere etterlevelsen av regelverket i virksomheten. Dette skal samlet bidra til at alle krav i loven blir ivaretatt på en effektiv måte og at virksomheten har prosesser for å sikre kontinuerlig forbedring over tid. Dokumentasjon av internkontroll skal være tilgjengelig for ansatte og andre som utfører oppgaver for virksomheten, eventuelle databehandlere og for Datatilsynet.

Internkontrollen skal fungere som ledelsens verktøy for å gi rammer og føringer som bidrar til lik praktisering internt i virksomheten. For den enkelte ansatte skal internkontrollen bidra til at det er enkelt å gjøre de daglige arbeidsoppgavene riktig.

Nærmere beskrivelse av innholdet og eksemplifisering av disse tre delene av internkontrollen er illustrert i figuren nedenfor.



Styrende dokumentasjon	• Skal beskrive internkontrollsystemet og målsettingen med det. Skal fungere som et bindeledd mellom kravene i lov og forskrift, interne krav og virksomhetens prosesser og dokumentasjon. • Skal blant annet inneholde oversikt over rolle- og ansvarsfordeling for å ivareta ulike plikter. Dette gjelder både ulike lederstillinger og nøkkelroller.
Gjennomførende dokumentasjon	• Skal beskrive hvordan informasjon skal behandles. Retter seg i hovedsak mot de ansatte og skal sikre at alle behandler personopplysninger i tråd med lovkrav samt instrukser og retningslinjer fra ledelsen. • Dette kan eksempelvis være rutine for hvem som er ansvarlig for å gi innsyn i opplysninger på forespørsel, og hva som skal gjøres og registreres hvor ved slike henvendelser. Et annet eksempel er beskrivelser av rutiner og prosess ved mottak av en begjæring om utlevering.
Kontrollerende dokumentasjon	• Skal beskrive hvordan ledelsen kan få bekreftet hvorvidt opplysninger behandles i tråd med føringer og krav i den styrende og gjennomførende dokumentasjonen. Dette innebærer også etablering av prosedyrer for oppfølging, og forbedring av ulike deler av internkontrollen over tid. • Skal bl.a. omfatte plan for stikkprøvekontroller, revisjoner, rutiner for melding om og oppfølging av avvik og planmessig gjennomgang av internkontrollen som gjøres jevnlig – eksempelvis som en del av et årshjul.

14.1 Personvern- og informasjonssikkerhetspolicy

14.1.1 Personvernpolicy

En personvernpolicy er en del av den styrende delen av internkontrollen. Innholdet vil typisk være å angi virksomhetens mål med personvernarbeidet, en oversikt over hvilke krav og plikter som påhviler virksomheten, strategi for å etterleve disse og fordeling av roller og ansvar for ulike oppgaver og aktiviteter som må ivaretas for å tilfredsstille kravene.

Personvernpolicy kan være et selvstendig dokument eller inngå i samme dokument som informasjonssikkerhetspolicy.

14.1.2 Informasjonssikkerhetspolicy

Formålet med informasjonssikkerhetspolicyen er å underbygge og støtte opp personopplysningslovens krav om tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. En informasjonssikkerhetspolicy skal inkludere sikkerhetsmål, sikkerhetsstrategi, og hva som skal gjøres for å nå målene herunder tilstrekkelig beskyttelse av informasjonsverdier mot alle identifiserte trusler (både interne og eksterne, samt tilsiktede og utilsiktede), etablere rutiner for å håndtere uønskede hendelser samt påse at medarbeidere som bruker virksomhetens informasjonssystemer har tilstrekkelig kompetanse for å ivareta virksomhetens sikkerhetsbehov.

14.2 Oversikt over behandlinger

Det er et krav om å etablere og vedlikeholde en oversikt over behandlinger av personopplysninger.[76]

I tillegg til å være et lovfestet krav for de fleste virksomheter, er slik oversikt nødvendig for å kunne ha oversikt og kontroll over eget ansvarsområde, slik at man kan ivareta sine plikter som

[76] *Se personvernforordningen artikkel 30.*

behandlingsansvarlig. Oversikten er videre et viktig utgangspunkt ved risikovurderinger, vurdering av personvernkonsekvenser og ved vurdering av nødvendige tiltak for å sikre kravene til innebygd personvern. Dette er bakgrunnen for at vi anbefaler å etablere en slik oversikt, selv om en virksomhet kan komme inn under bestemmelsen om fritak fra plikt til å etablere slik oversikt som følge av størrelsen på egen virksomhet.[77]

En slik oversikt over behandlinger må først etableres, deretter oppdateres ved oppstart av ny behandling eller andre endringer. Dette er typisk oppstart av nye prosesser, etablering av nye systemer, produkter eller tjenester. I tillegg anbefales det å gjøre en årlig gjennomgang, for å sikre at alle endringer som er utført i løpet av året, er fanget opp.

Det skal foreligge en vedlikeholdt oversikt over behandlinger av personopplysninger. Oversikten skal minimum inneholde følgende informasjon:

- Formålet med behandlingen
- Kategorier av registrerte og kategorier av personopplysninger
- Mottakere av opplysningene om informasjon utleveres
- Om det skjer en overføring av personopplysninger til tredjeland
- Tidsfrister for sletting av de ulike kategorier av opplysninger
- Om mulig, en generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak
- Navn og kontaktinformasjon på den behandlingsansvarlige og navn på eventuelt personvernombud

I tillegg anbefales å ta med følgende elementer når det først skal opprettes en slik oversikt over behandlinger:

- Behandlingsgrunnlag for behandlingen
- Kilder til informasjon som samles inn og registreres
- Bruk av databehandlere

En mal for oversikt over behandlinger er tilgjengelig via Energi Norges nettsider. Denne kan tilpasses til bruk i egen virksomhet.

14.3 Kontrollerende og korrigerende prosesser

14.3.1 Egenkontroller og gjennomganger

Det er viktig å etablere regelmessig gjennomgang av egne dokumenter og prosesser. Formålet med slike gjennomganger er å sikre at dokumentasjon og prosesser er hensiktsmessig og dekkende for faktiske behov som virksomheten har. Slik regelmessig egenkontroll bør gjennomføres minst årlig.

I tillegg skal virksomheten gjennomføre en gjennomgang av internkontroller der formålet er å avdekke eventuelle hull og svakheter i etterlevelsen av etablerte rutiner. Det bør minst årlig gjennomføres en systematisk gjennomgang av om iverksatte tiltak fungerer etter sin hensikt slik at

[77] *Se personvernforordningen artikkel 30 pkt. 5*

behov for forbedringer kan identifiseres og justering i tiltak, kan settes i verk. Dette er typisk en gjennomgang av selve internkontrollsystemet; både hvordan det er bygget opp og hvordan det fungerer i praksis. En slags «indremedisinsk» gjennomgang for deretter å kunne tilpasse dokumentasjon og prosesser til det reelle behovet. Dette kan gjøres gjennom å undersøke om siste versjoner av dokumentasjon er tilgjengelig for de som trenger det i sitt arbeid, om dokumentene er forståelige, om de oppdateres ved behov, om det gjennomføres opplæring, at alle kjenner sin rolle og ansvar, om det iverksettes tiltak når det identifiseres behov og om tiltakene faktisk passer behovet.

Resultatet bør inngå i en oppsummering som fremlegges og gjennomgås hos virksomhetens ledelse på jevnlig basis, se eget punkt om ledelsens gjennomgang.

En slik egenkontroll kan blant annet inkludere sjekk av om:

- Rutine for godkjenning av nye systemer, prosjekter, produkter og rutine for godkjenning av applikasjoner og oppgraderinger er tilstrekkelig kjent for roller som er eller skal være involvert
- Rutiner for å ivareta rettigheter til den registrerte er oppdaterte og fulgt opp
- At avvik meldes internt og videre til Datatilsynet når nødvendig
- Om oversikt over databehandler er oppdaterte og at disse faktisk er fulgt opp i avtaleperioden
- Rutiner for sletting følges

Sentrale aktiviteter i forbindelse med kontroller kan omfatte følgende steg:

- Peke ut den som skal ha rollen som ansvarlig for gjennomgangen
- Utarbeide en plan som viser hva som skal gjennomgås og tidspunktet for gjennomføring
- Ha dialog med de enhetene som har ansvaret for området som skal gjennomgås om fremleggelse av relevant dokumentasjon osv.
- Bestemme hva slags undersøkelser man skal gjennomføre, f.eks. stikkprøver og andre kontroller
- Utarbeide en rapport med forslag til forbedringer
- Gi de som er berørt av gjennomgangen mulighet til å uttale seg om eventuelle funn og forslag til forbedringstiltak
- Overlevere resultater til ledelsen

14.3.2 Ledelsens gjennomgang

Virksomhetens ledelse bør minst en gang i året gjennomgå status for hvordan internkontrollen i sin virksomhet fungerer og identifisere forbedringsbehov og prioritere iverksettelse av tiltak. Ledelsens gjennomgang er viktig med å tanke på å sikre planlagt og systematisk rapportering av status innen etterlevelse av personopplysningsloven for å understøtte kontinuerlig forbedring. Herunder ta stilling til hvorvidt man skal:

- Utbedre lederbekreftelser til flere og mer konkrete spørsmål for å fange opp faktisk situasjon innen personopplysningsområdet.
- Vurdere ytterligere aktiviteter innen egenkontroll og andre kontrolltiltak innen personopplysningsloven.
- Synliggjøre status i etterlevelse av personopplysningsloven bedre i kvartals- og årsrapporter.

Slik gjennomgang kan med fordel være felles med rapportering innen informasjonssikkerhet.

Tips: **Forslag til underlag for ledelsens gjennomgang:**	
Avviksrapportering	• Omfang avviksrapportering i forrige periode. • Fordeling av avvik på tema/områder. • Kommentarer til de mest alvorlige avvikene, gjengangere e.l.
Virksomhetens egenkontroll	• Er gjennomgang av hele eller deler av internkontrollen gjennomført? For eksempel gjennomgang av tilgangsrettigheter? • Sentrale funn herfra og eventuelle identifiserte tiltaksbehov
Revisjonsrapport(er)	• Er revisjon av hele eller deler av internkontrollen gjennomført? • Sentrale funn herfra og eventuelle identifiserte tiltaksbehov?
Funn fra gjennomførte risikovurderinger eller personvern-konsekvensvurderinger	• Hvor mange vurderinger er gjennomført siden forrige gjennomgang med hvilke tema? • Er det identifisert mange tiltaksbehov og hva er det viktigste, mest sentrale? (Typisk som krever evt. investering eller tilgang til flere ressurser). • Andre viktige erfaringer det er grunn til å nevne her?
Evt. tilsynsrapporter	• Har dere hatt tilsynsbesøk fra Datatilsynet? Andre i næringen? • Kort oppsummering av resultatet og eventuelle funn og pålegg om utbedring derfra
Endring i krav mv.	• Er det noen nye lov- eller forskriftskrav som vil stille krav til hvordan oppgaveløsningen skal være? • Sentrale instrukser veiledere eller noe som på annen måte som gir føringer som det er grunn til å nevne her?
Endringer i trusselbildet	• Har det skjedd noen markante endringer av trusselbildet som tilsier iverksettelse av tiltak?
Annet	• Rapporter fra IKT- avdelingen • Status på tiltak fra ledelsens gjennomgang sist år • Status innen sikkerhetskultur i virksomheten.

15. Opplæring

Ansatte må gis opplæring i hvordan krav til personvern og informasjonssikkerhet skal ivaretas. Målet med opplæring er å sørge for at ansatte i virksomheten er oppmerksomme på trusler mot personvern og informasjonssikkerheten generelt, og legge til rette for å etterleve fastsatte krav til deres daglige arbeid. Det innebærer blant annet opplæring i riktig bruk av informasjonssystemer for å redusere potensielle sikkerhetsrisikoer. Dette krever aktiviteter rettet mot å heve kunnskap, bevisstgjøring og forbedre ferdigheter.

Opplæring bør tilpasses den enkeltes rolle og på hvilken måte vedkommende er i kontakt med kunder, ansatte eller disses personopplysninger gjennom sine oppgaver i virksomheten. Ved å forklare på en forståelig måte hvorfor informasjonssikkerhet er viktig i deres arbeidshverdag, legger man til rette for en god sikkerhetskultur i virksomheten, som er helt nødvendig for å sikre tilstrekkelig etterlevelse og forbedring av krav og sikkerhetstiltak.

Det anbefales å variere bruk av ulike virkemidler som for eksempel kurs, foredrag, e-læringskurs, plakater osv. Det gir erfaringsvis bedre effekt å bruke ulike typer virkemidler og kanaler fordi det varierer fra person til person hvilke virkemidler som treffer. Det er videre viktig at opplæring kombineres med jevnlige påminnelser som bidrar til at bevisstheten om hva som kreves av tiltak og hvorfor opprettholdes også over tid. Slike aktiviteter bør i tillegg til å tilpasses den enkeltes rolle også tilpasses ansettelsessyklusen (oppstart, endring av rolle, opphør).

Før ansatte i organisasjonen får tilgang til informasjon eller tjenester, bør de få hensiktsmessig opplæring. Dette omfatter bl.a. opplæring i:

- De juridiske plikter som bedriften har overfor sine kunder og ansatte, herunder
- Orientering om omfanget av taushetsplikten
- Hva som er riktig håndtering av forespørsler fra den enkelte som de ansatte vil kunne motta, slik at de henvendelser som måtte komme, blir håndtert på en riktig og effektiv måte
- Hva som er korrekt bruk av systemer som behandler personopplysninger,
- Forventning til den enkelte for ivaretakelse av informasjonssikkerhet, forståelse av aspektene integritet, konfidensialitet og tilgjengelighet.
- Hvilke regler som gjelder bruk av e-post.
- Viktigheten av rapportering av avvik for å sikre kunnskap om og omforent forståelse av hvilke hendelser som skal rapporteres og hvorfor.

I tillegg bør de få regelmessig oppdatering i hvilke instrukser og andre føringer som gjelder og ny tilpasset opplæring ved skifte av rolle i internt eller endringer i hvordan prosessene skal utføres. Tilsvarende opplæring bør vurderes for vikarer og konsulenter. Det samme gjelder tredjeparter som enten har tilgang til virksomhetens systemer eller utfører oppgaver på vegne av virksomheten.

Det bør dokumenteres at opplæring er gitt, både når hvilke opplæringstiltak er gjennomført og hvem som har deltatt.

16. Tilslutning, kontroll, klage mv

16.1 Tilslutning til bransjestandard

Bransjestandarden gir anvisning på god praksis for etterlevelse av krav til personvern og er et uttrykk for en felles forståelse i bransjen for hva som er tilfredsstillende nivå for etterlevelse på de områder som er omtalt. Bransjestandarden er veiledende for alle virksomheter, herunder leverandører. Hvorvidt en virksomhet bestreber seg på å etterleve standarden, kan gis som informasjon på virksomhetens egen nettside eller på annen egnet

16.2 Kontroll med overholdelse

Det er ikke utpekt et eget organ innad i bransjen for utøvelse av kontroll med etterlevelsen av bransjestandarden. Kontroll av etterlevelse av forordningens krav utøves dermed kun av Datatilsynet ut fra den kompetanse som er tillagt tilsynet gjennom personvernforordningen.[78]

16.3 Klagehåndtering

Om en registrert person vil klage på den behandling av personopplysninger som finner sted, har vedkommende mulighet til å klage til behandlingsansvarlig virksomhet, direkte til eventuelt personvernombud i virksomheten eller til Datatilsynet. Det skal gis veiledning om slik klageadgang til den registrerte, f.eks. i en personvernerklæring.

16.4 Endringer

Utarbeidelse av denne bransjestandarden har skjedd gjennom samarbeid mellom flere virksomheter i bransjen. Mange virksomheter har deltatt i arbeidsmøter og det har vært høringsrunder i bransjen. Energi Norge har vært pådriver og tilrettelegger.

Bransjestandarden vil måtte tilpasses eventuelle endringer i lovverket eller praktiseringen som følge av avklaringer fra Datatilsynsmyndigheter mv som er relevante for bransjens behandling av personopplysninger. Energi Norge har ansvaret for at bransjestandarden til enhver tid er i tråd med det gjeldende regelverket for bransjen. Dette dokumentet vil bli oppdatert jevnlig ved behov. Energi Norge setter pris på innspill og tilbakemeldinger om mulige forbedringsområder.

[78] *Se personvernforordningen artikkel 57 og 58*

Vedlegg

Vedlegg 1: Sentrale begreper og oversikt over kilder

Vedlegg 2: Klassifisering

Vedlegg 3: Mal for personvernkonsekvenser (DPIA)

Vedlegg 4: Liste over personvernscenarioer

Vedlegg 5: Sjekkliste for avtaler

Vedlegg 1. Sentrale begreper og oversikt over kilder

AMS	”Avanserte Måle- og Styringssystemer” (AMS). Innebærer at brukerne får informasjon om strømforbruket sitt, mer nøyaktig avregning og mulighet for automatisk styring av forbruket.
	Les mer: Informasjon om AMS fra RME: https://www.nve.no/stromkunde/smarte-strommalere-ams/ Veileder til sikkerhet i avanserte måle- og styringssystem: https://www.nve.no/Media/5525/veiledertil-sikkerhet-i-ams.pdf Datatilsynets oversikt over krav ved behandling av personopplysninger fra AMS-målere: https://www.datatilsynet.no/rettigheter-og-plikter/overvaking-og-sporing/strommaling/
Avvik	Dette kan for eksempel være alt fra tyveri av bærbart utstyr, bruker som går fra arbeidsstasjonen usikret, bruker låner ut brukernavn og passord til andre, forsøk på å sende sensitive personopplysninger i e-post/vedlegg, misbruk/angrep på IKT-systemer og andre feil og uhell som følge av menneskelige feil eller som følge av brann og vannlekkasjer. Definisjon i personvernforordning artikkel 4: «brudd på personopplysningssikkerheten» et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.»
Behandling av person-opplysninger	All bruk av personopplysninger, det vil si all innsamling, registrering, strukturering, lagring, tilpasning, søk, gjenfinning, bruk, utlevering, overføring, tilgjengeliggjøring, sammenstilling mv. som gjøres frem til at opplysningen er slettet endelig. Både registrering av opprettelse av kundeforhold, registering og bruk av strømforbruk, betalingshistorikk med videre om kunder er behandlinger av personopplysninger. Definisjon i personvernforordning artikkel 4: ««behandling» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. 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.»
Behandlings-ansvarlig	Den som bestemmer formålet med behandlingen og hvilke virkemidler som skal benyttes ved oppgaveløsingen. Dette vil normalt være øverste leder i den aktuelle juridiske virksomheten. Formål med aktuelle behandlinger kan også ofte leses ut fra beskrivelse i den lov eller forskriften som regulerer aktuell behandling. Definisjon i personvernforordning artikkel 4: ««behandlingsansvarlig» 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 midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett.»

Behandlings-grunnlag	Behandlingsgrunnlag er et rettslig grunnlag for å behandle personopplysninger. Dette kan typisk være et samtykke, kundeavtale eller hjemmel i lov. Kalles av og til også for «rettsgrunnlag» eller «hjemmelsgrunnlag».
Databehandler	En tredjepart som behandler personopplysninger på vegne av virksomheten. Dette kan typisk være en driftsleverandør som drifter et eller flere IT-systemer og i den forbindelse har adgang til personopplysninger om ansatte eller kunder. Definisjon i personvernforordning artikkel 4: ««databehandler» en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige.» Databehandler er alltid en aktør utenfor den behandlingsansvarliges egen organisasjon.
DPIA	Se «Personvernkonsekvensvurdering»
GDPR	General Data Protection Regulation. EU forordning som erstattet personverndirektivet 95/46/EF og innført i norsk rett fra 20. juli 2018.
	Les mer: Lenke til lovdata: https://lovdata.no/dokument/NL/lov/2018-06-15-38?q=personopplysningsloven Original ordlyd: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL Lenke til oversikt utarbeidet av Datatilsynet om hva loven har å si for en bedrift og hvilke tiltak som bør gjøres: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/grunnleggende-personvernprinsipper-etter-nytt-regelverk/
Gjennom-fakturering	Strømleverandør fakturerer sluttbruker for nettjenester og elektronisk energi felles ved at faktura for nettjenester sendes fra nettselskapet til sluttbrukerens strømleverandør, som betaler på vegne av sluttbruker.
HAN-port	HAN står for «Home Area Network» Alle AMS-målere er utstyrt med en fysisk utgang, kalt HAN-porten. Gjennom å koble seg til HAN-porten vil kunden få tilgang til informasjon om eget strømforbruk. Informasjonen vil kun være tilgjengelig for kunden, verken nettselskap, kraftleverandører eller tjenesteleverandører har leseadgang til HAN-porten. Disse, og eventuelt andre aktører, kan kun få tilgang til disse dataene etter avtale med kunden. Porten vil være stengt når den nye måleren installeres, og vil bare kunne åpnes når kunden ber om det.
	Les mer: Informasjon om alle elektrotekniske standarder finnes her: https://www.nek.no/
Informasjons-sikkerhet	Informasjonssikkerhet handler om å beskytte informasjon og miljøet hvor informasjonen behandles mot uønskede hendelser og handlinger. Dette innebærer at informasjon beskyttes mot uautorisert innsyn (konfidensialitet), uautorisert endring (integritet) og at den er tilgjengelig når det er behov for den (tilgjengelighet).

Person-opplysninger	Alle opplysninger som kan knyttes til en identifiserbar enkeltperson, direkte eller indirekte. Det er ikke avgjørende at enkeltperson faktisk er identifisert, men at det er mulig å knytte opplysninger opp til en bestemt person. Det er både den behandlingsansvarliges og andres mulighet for å identifisere som må vurderes. Dette innebærer at f.eks. navn, adresse, telefonnummer etc., men også IP-adresser kan være personopplysninger. Det samme gjelder målernummer eller målepunkt ID på en adresse som kan knyttes til en huseier eller leietaker. Opplysninger om atferdsmønstre er også å regne som personopplysninger. Detaljerte data om strømforbruket kan si noe om både vaner og tilstedeværelse, gjøremål mv. Det må derfor alltid gjøres en konkret vurdering av et informasjonselement er egnet til å utlede noe om en enkeltperson, enten alene eller sammen med annen informasjon som er tilgjengelig. Om opplysningene er å anse som en personopplysning, innebærer det plikt til å påse at lovens krav er oppfylt ved behandlingen, herunder krav om tilfredsstillende informasjonssikkerhet. Er det reelt sett anonyme opplysninger som foreligger, faller behandling av slike opplysninger utenfor personopplysningslovens virkeområde. Definisjon i personvernforordning artikkel 4: «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar 33 fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en online-identifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet.»
Personvern-konsekvens-vurdering	En systematisk prosess, som identifiserer og evaluerer potensielle personvernkonsekvenser fra alle interessenters synsvinkel i et prosjekt, initiativ, foreslått system eller prosess. Den skal benyttes på nye produkter, tjenester, systemer. Det er særlig aktuelt å gjøre en slik vurdering når det tas i bruk ny teknologi. Vurderingen inkluderer å finne ut hvordan man kan unngå trusler mot personvernet eller hvilke tiltak som må innføres for å avverge trusler mot personvernet. Bestemmelsene knyttet til vurdering av personvernkonsekvenser står i artikkel 35 i den nye forordningen for personvern.
	Les mer: Veileder fra Datatilsynet: https://www.datatilsynet.no/regelverk-og-skjema/veiledere/vurdering-av-personvernkonsekvenser2/
Risikovurdering	En risikovurdering er et verktøy for å identifisere uønskede hendelser og risikoen for at disse skal inntreffe - en vurdering av risiko ved brudd på sikring av konfidensialitet, integritet og tilgjengelighet.
	Les mer: Veileder fra Datatilsynet: https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/risikovurdering/ Se vedlegg 3 om introduksjon til praktisk risikoanalyse i «Veileder om økonomisk kriminalitet i energibransjen» som har god overføringsverdi til risikoanalyser innen informasjonssikkerhet. Andre eksempler på ROS-analyser mv: https://www.nve.no/damsikkerhet-og-energiforsyningsberedskap/energiforsyningsberedskap/regelverk-og-skjema/
Sensitive person-opplysninger	Definisjon i personopplysningsloven av 2001: «sensitive personopplysninger: opplysninger om a) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, b) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling, c) helseforhold, d) seksuelle forhold, e) medlemskap i fagforeninger.» Denne definisjonen er erstattet med en definisjon av «særlige kategorier», se nedenfor.

Særlige kategorier av person-opplysninger	Opplysninger knyttet til rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, genetiske og biometriske opplysninger, helseopplysninger og seksuelle forhold eller seksuell orientering. Det er også særskilt lovregulering av behandling av personopplysninger om straffedommer og lovovertredelser. For kraftnæringen er det særlig helseopplysninger det kan oppstå problemstillinger for, typisk der det er helsemessige årsaker til at strøm ikke kan stenges av, helsemessige krav til visse funksjoner mv, ansatte som har åpen soning eller begrunnelse for velferdspermisjoner. Definisjon i artikkel 9 nr 1: «Opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, 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.»
Styringssystem for informasjons-sikkerhet	Styringssystem for informasjonssikkerhet skal sikre at arbeidet med personvern og informasjonssikkerhet blir en kontinuerlig prosess og ivaretatt på en systematisk og dokumentert måte.
Samtykke	Et gyldig samtykke skal være avgitt frivillig, det skal være spesifikt, den registrerte skal være informert om alle relevante konsekvenser ved å gi sitt samtykke i en forståelig og lett tilgjengelig form og viljeserklæringen skal være utvetydig/aktivt. Det siste krever at det gjøres en handling for å bekrefte et valg. Forhåndsutfylte bokser og mangel på reelt valg er dermed ikke tilstrekkelig. Det er heller ikke tilstrekkelig å operere med passive samtykker som krever at kunden må si ifra om han ikke ønsker den aktuelle tjenesten. Kravet til frivillighet innebærer at samtykke er lite egnet til alle formål i arbeidslivet. Til det er ubalansen i styrkeforholdet mellom arbeidsgiver og arbeidstaker for stor. Det skal videre være enkelt å trekke tilbake samtykker og den enkelte skal være informert om at det kan trekkes tilbake. For eksempel kreves det samtykke fra kunden før det er aktuelt å benytte HAN-porten i smarte strømmålere til andre formål. Definisjon i personvernforordningen art. 4: ««samtykke» fra den registrerte enhver frivillig, spesifikk, informert og utvetydig viljesytring fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende.»

Vedlegg 2. Klassifisering

Konfidensialitetsklasse *Beskrivelse av hvilken grad av beskyttelse som kreves for informasjon for å unngå at de er tilgjengelige for uvedkommende*	
Åpen	Informasjonen kan eller skal være tilgjengelig for alle uten pålogging/særskilte tilgangsrettigheter. *Eksempel på slik informasjon kan være websider og annet materiell som legges åpent ut på internett.*
Intern	Informasjonen er tilgjengelig for utvalgte interne og eksterne brukere, men krever pålogging/kontrollerte tilgangsrettigheter. *Eksempel på slik informasjon er personopplysninger og arbeidsdokumenter.*
Fortrolig	Informasjonen krever streng tilgangsstyring. Klassifiseringen benyttes hvis offentliggjøring vil skade offentlige interesser, institusjonen eller enkeltperson(er). *Eksempel på slik informasjon kan være store mengder særlige kategorier personopplysninger, som for eksempel helseopplysninger.*
Strengt fortrolig	Informasjonen krever meget streng tilgangsstyring. Klassifiseringen benyttes hvis offentliggjøring vil gi betydelig skade på offentlige interesser, institusjonen eller enkeltpersoner. *Beskyttelse av personer med Kode 6, er et eksempel her.*
Integritetsklasse *Beskrivelse av hvor viktig det er at informasjonen ikke kan endres av uvedkommende eller ved et uhell*	
Lave krav til integritet	Informasjonen ligger ikke til grunn for beslutninger. Handlinger basert på eventuelle feil informasjonen kan enkelt rettes opp og vil normalt sett ikke medføre konsekvenser av økonomisk, omdømmemessig eller personlig art. *Eksempel på sikringstiltak er en-faktor autentisering.*
Middels krav til integritet	Den som benytter informasjonen forventer at den er autentisk og gyldig. Feil i informasjonen kan gi moderate økonomiske skader og/eller svekket omdømme for virksomheten, enkeltindivider eller samarbeidspartnere. *Eksempel på sikringstiltak er to-faktor autentisering.*
Høye krav til integritet	Den som benytter informasjonen er avhengig av at den er autentisk og gyldig. Utilsiktet eller tilsiktet feilinformasjon vil kunne føre til feilvurderinger eller beslutninger slik at det kan medføre betydelig økonomisk tap, omdømmetap eller annen skade for virksomheten, enkeltindivider eller samarbeidspartnere. *Eksempel på sikringstiltak er to-faktor autentisering, skrivebeskyttelse, digital signering og logging.*
Tilgjengelighetsklasser *Beskrivelse av hvor lenge man kan akseptere at informasjonen er utilgjengelig. Noen systemer og tjenester er kritiske for at virksomheten skal kunne utføre sine oppgaver*.	
Lave krav til tilgjengelighet:	Informasjonen kan være utilgjengelig i lengre perioden uten at dette medfører konsekvenser av betydning for virksomheten eller enkeltpersoner. Informasjon som går tapt kan relativt enkelt gjenskapes via andre kilder, internt eller eksternt.
Middels krav til tilgjengelighet:	Dersom informasjonen er utilgjengelig kan dette redusere produksjonen med hele eller deler av virksomheten og/eller ha visse konsekvenser av økonomisk art, for virksomhetens omdømme, enkeltpersoner og/eller samarbeidspartnere. Informasjon som går tapt kan gjenskapes, men det krever betydelig ressursbruk og/eller skaper store forsinkelser.
Høye krav til tilgjengelighet:	Selv korte avbrudd kan få store konsekvenser for enkeltpersoner, samarbeidspartnere, virksomhetens omdømme eller økonomi. Informasjon som går tapt kan ikke gjenskapes og dette kan få store konsekvenser for virksomhetens oppgaver, omdømme, økonomi og få konsekvenser for enkeltpersoner.

Vedlegg 3. Mal for personvernkonsekvenser (DPIA)

Hva er hensikten med malen?
En vurdering av personvernkonsekvenser skal sikre at personvernet til de registrerte blir ivaretatt.
Å gjennomføre en personvernkonsekvensvurdering skal bidra til at virksomheten:

- Håndterer risikoer behandlingen innebærer for den registrerte nå og i fremtiden (til forskjell fra risiko for den enkelte virksomhet)
- Identifiserer behov for risikoreduserende tiltak
- Demonstrere og dokumentere ansvarlighet ovenfor ledelsen, Datatilsynet, evt. personvernombudet og de registrerte

Dokumentasjon og ajourhold

Grunnleggende informasjon	
Tema/område/formål	
Risikoeier	
Vedlegg	(Legg til evt vedlegg som kan gi utdypende informasjon)
Referanse til lagringssted av vurderingene og annen dokumentasjon	

Deltagere		
Navn	Rolle	Enhet

Eksterne deltagere	
Representant for brukere	
Representant for databehandler	
Begrunnelse for evt. manglende involvering av eksterne:	

Endringslogg		
Dato for første versjon		
Evt. dato for oppdatering	Endringer	Godkjent av eier

1. Behandlingen av personopplysninger

Overordnet oversikt over behandlingen Gi en kort, overordnet presentasjon av denne behandlingen.	
Hvorfor behandle personopplysninger? Hva er formålet med behandlingen?	
Eventuelle avgrensninger for denne vurderingen	
Gi en beskrivelse av behandlingens livsløp (steg for steg). Flytdiagram kan med fordel brukes.	

Behandlingens art og omfang	
Hvem skal det samles inn personopplysninger om?	
Hvilke kategorier av personopplysninger skal behandles? *(Personalia, adresse/ kontaktinfo/Helseopplysninger/ Logger/økonomiske opplysninger/annet?)*	
Hvor mange brukere er omfattet?	(Ca. antall er tilstrekkelig)
Hvordan er utvalget bestemt?	-

Behandlingens nødvendighet og proporsjonalitet	
• Behandlingen må være nødvendig – derfor må det vurderes om behandlingen kan gjennomføres på en annen eller mindre inngripende måte. • Det skal være et rimelig forhold mellom det inngrepet som gjøres i personvernet og de fordeler som oppnås ved behandlingen av personopplysninger.	
Beskriv vurderingene og avveiingene som er gjort:	

2. Relaterte krav og prosesser

Behandlingsoversikt			
Er behandlingsaktiviteten allerede beskrevet i virksomhetens behandlingsoversikt?	☐ Ja	☐ Nei	☐ Delvis
Hvis ja – gi referanse til behandlingen			
Hvis nei eller delvis, angi hvem som sørger for å oppdatere og når dette forventes utført			

Rettslig grunnlag	
For å sikre at behandlingen er lovlig, trengs en nærmere beskrivelse av det rettslige grunnlaget for den spesifikke behandlingen.	
Hva er det rettslige grunnlaget for denne behandlingen?	

Risikovurdering	
Det skal gjennomføres en risikovurdering av informasjonssikkerheten tilknyttet personopplysningene, det som i personopplysningsloven kalles personopplysningssikkerheten.	
Referanse til relevante risikovurderinger (lenke eller vedlegg)	

3. Konsekvenser for den enkelte

I dette steget skal man identifisere og vurdere aktuelle personvernkonsekvenser basert på flere scenarioer. Det er viktig å ta perspektivet til de registrerte og vurdere hvordan behandlingen kan påvirke deres personvern.

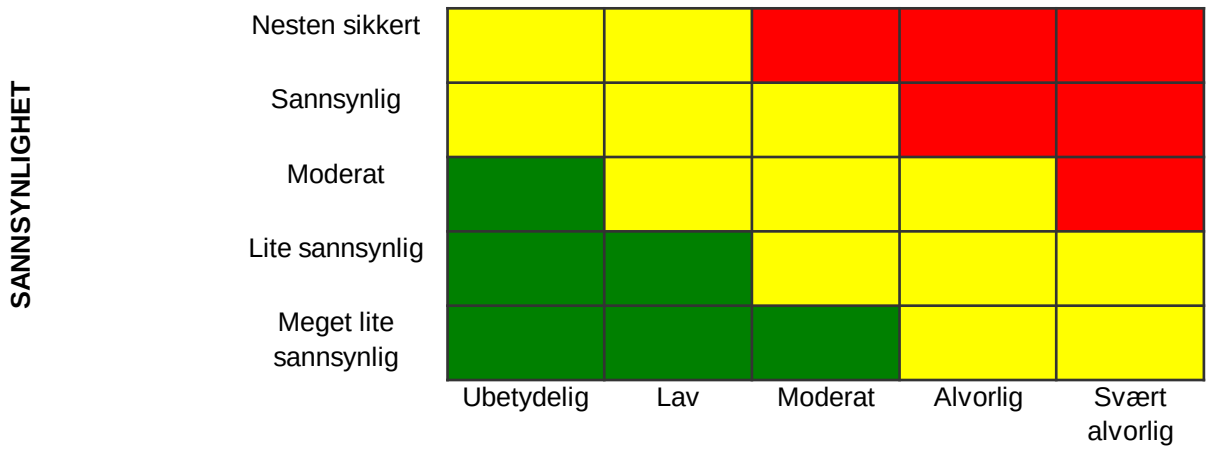
Relevante scenario

Sett inn personvernscenario er vurdert som relevante i vurderingen av personvernkonsekvenser. For inspirasjon, vises det til vedlegg 4 i Veileder og bransjestandard for personvern i energibransjen.

1) Beskriv scenariet - tilpasset det som er relevant for den aktuelle behandlingen
2) Beskriv gjerne en kort begrunnelse for valgt sannsynlighets- og konsekvensnivå
3) Sett deretter inn fastsatt sannsynlighet- og konsekvensnivå for den aktuelle behandlingen.

Nr	Personvernscenario	Konsekvens	Sannsynlighet
1		2	5
2		2	4
3		4	5
4		2	5
5		2	3
6		2	5
7		3	1
8		3	1
9		3	1
10		Velg et nivå.	Velg et nivå.
11		Velg et nivå.	Velg et nivå.

Risikobilde før tiltak
Plott inn hvor de ulike scenarioene vil befinne seg etter at tiltakene fra tabellen over er gjennomført. Det er dette risikobildet risikoeier må vurdere om kan aksepteres eller ikke.



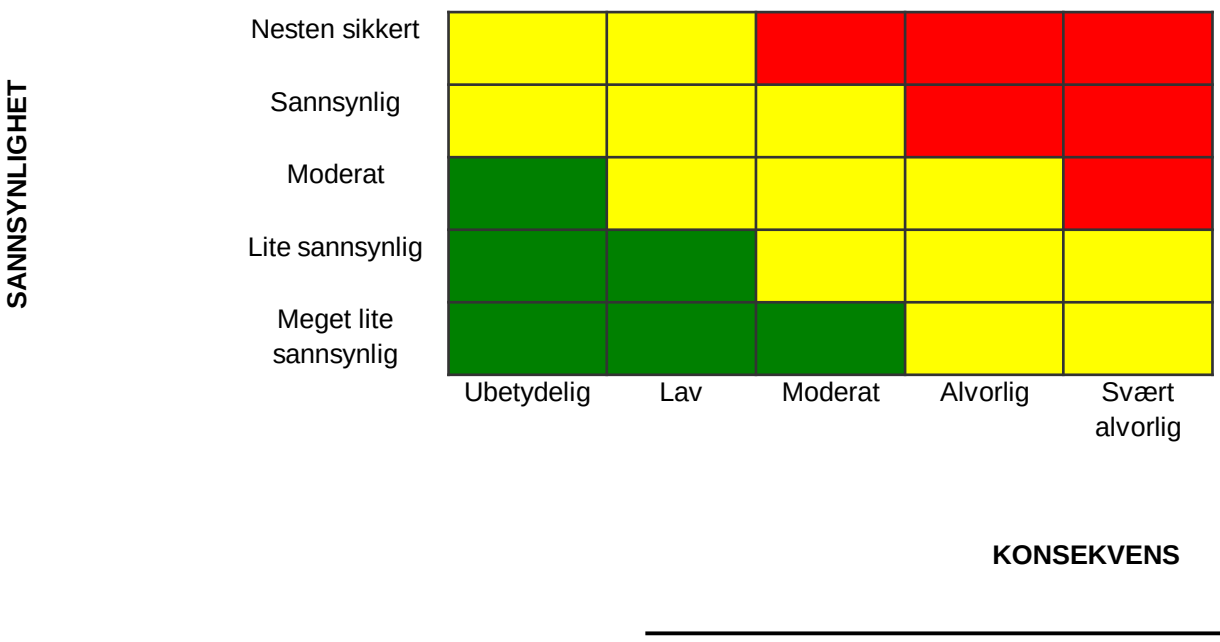
4. Tiltak

4.1 Tabell for risikoreduserende tiltak

Tiltak			
Tabellen oppdateres etter vedlegg 1 er gjennomgått og tiltak er bestemt.			
Risikoreduserende tiltak	For hvilke(t) scenario?	Ansvarlig	Frist

4.2 Risikobilde etter tiltak

Plott inn hvor de ulike scenarioene vil befinne seg etter at tiltakene fra tabellen over er gjennomført. Det er dette risikobildet risikoeier må vurdere om kan aksepteres eller ikke.



5. Avslutning

5.1 Vurdering og råd fra personvernombudet (Om virksomheten har dette)

Personvernombudet skal gi sine råd og anbefalinger for å beskytte de registrertes personvern før endelig godkjenning hos risikoeier.

Personvernombud		
Spørsmål for personvernombudet	Tilstrekkelig?	Kommentarer
Personvernscenarioene slik de er beskrevet?	☐ Ja ☐ Nei	
Risikoreduserende tiltak	☐ Ja ☐ Nei	
Andre tilbakemeldinger		
Anbefaler personvernombudet at arbeidet går videre som planlagt? Eventuelt behov for å fremme saken til forhåndskonsultasjon til Datatilsynet?		

5.1 Endelig godkjenning

Endelig godkjenning			
Vurderingen skal godkjennes av risikoeier. Eventuell restrisiko er akseptert ved godkjenning.			
Er anbefalinger fra PVO fulgt?	☐ Ja		☐ Nei
Dersom nei, hvorfor ikke?			
Er vurderingene av personvernkonsekvens i sin helhet godkjent?	☐ Ja		☐ Nei
Dato		Signatur	

Beskrivelse av sannsynlighet- og konsekvensnivå

Sannsynlighetsnivå		
Nivå	**Beskrivelse**	**Veiledning**
1	Meget lite sannsynlig	Mindre enn 10 % sannsynlig og/eller inntreffer hvert 5. år eller sjeldnere
2	Lite sannsynlig	10-30 % sannsynlig og/eller inntreffer hvert år eller sjeldnere
3	Moderat sannsynlig	30-60 % sannsynlig og/eller inntreffer 2-4 ganger per år
4	Sannsynlig	60-90 % sannsynlig og/eller inntreffer månedlig
5	Nesten sikkert	Over 90 % sannsynlig og/eller inntreffer ukentlig

Konsekvensnivå		
Nivå	**Beskrivelse**	**Veiledning**
1	Konsekvensen for den registrertes personvern er ubetydelig	• Forbigående, mindre økonomisk tap for den registrerte • Midlertidig og begrenset tap av den registrertes omdømme • Den registrertes rett til personvern utfordres i en svært kort periode og uten å involvere særlige kategorier/sårbare grupper
2	Konsekvensen for den registrertes personvern er lav	• Midlertidige eller mindre alvorlige helsemessige konsekvenser for den registrerte • Forbigående økonomisk tap for den registrerte • Midlertidig eller begrenset tap av den registrertes omdømme • Den registrertes rett til personvern utfordres i en kort periode eller uten å involvere særlige kategorier/sårbare grupper • Den registrertes tillit til virksomheten utfordres midlertidig
3	Konsekvensen for den registrertes personvern er moderat	• Midlertidige eller noe mer alvorlige helsemessige konsekvenser for den registrerte • Økonomisk tap av noe varighet for den registrerte • Midlertidige eller noe mer alvorlige tap av den registrertes omdømme • Den registrertes rett til personvern krenkes i en større periode eller involverer særlige kategorier/sårbare grupper • Den registrertes tillit til virksomheten utfordres
4	Konsekvensen for den registrertes personvern er alvorlig	• Varige eller alvorlige helsemessige konsekvenser for den registrerte • Økonomisk tap av betydelig varighet for den registrerte • Varig eller alvorlig tap av den registrertes omdømme • Den registrertes rett til personvern krenkes alvorlig i en større periode og involverer særlige kategorier/sårbare grupper • Den registrerte taper tilliten til virksomheten
5	Konsekvensen for den registrertes personvern er svært alvorlig	• Tap av liv for den registrerte • Varige og alvorlige helsemessige konsekvenser for den registrerte • Varig og betydelig økonomisk tap for den registrerte • Varig og alvorlig tap av den registrertes omdømme • Den registrertes rett til personvern krenkes på en svært alvorlig måte • Den registrerte og samfunnet taper tilliten til virksomheten

Vedlegg 4. Liste over mulige personvernscenarioer

Eksempler på personvernscenarioer sortert etter personvernprinsipp		
Personvernscenario	Beskrivelse	Eksempler på spissede personvernscenarioer
Lovlig		
Behandlingen av personopplysninger er ikke lovlig	Behandlingen av personopplysninger må ha et rettslig grunnlag for å være lovlig, og behandlingen må ikke gå utover det rettslige grunnlaget. Dette gjelder også ved utlevering og gjenbruk av personopplysninger.	• Behandlingen går utover det rettslige grunnlaget. <u>Gjenbruk</u> • Gjenbruk av personopplysninger medfører at behandlingen går utover det rettslige grunnlaget. <u>Utlevering</u> • Personopplysninger overføres til tredjepart uten at det foreligger behandlingsgrunnlag. • Det rettslige grunnlaget dekker kun egne formål, ikke utlevering. <u>Samtykke</u> • Samtykket oppfyller ikke kravene til et gyldig samtykke. • Det er ikke hentet inn samtykke for hver behandling. • Det skilles ikke mellom hvilke personopplysninger som er nødvendige for å oppfylle en avtale og hvilke opplysninger som er basert på samtykke. • Samtykke dekker ikke statistikk- og analyseformål. <u>Automatiserte avgjørelser</u> • Automatisk behandling har ikke et gyldig behandlingsgrunnlag.

Gjennomsiktighet		
Den registrerte får ikke tilstrekkelig informasjon om hvordan personopplysningene behandles og hva de skal brukes til.	Behandlingen av personopplysninger skal være oversiktlig og forutsigbar for den opplysningene gjelder. For å ivareta denne rettigheten må den registrerte får tilstrekkelig informasjon om behandlingen.	• Den registrerte får ikke eller har ikke tilgang til informasjon om behandling av personopplysninger. • Det gis ikke presis nok informasjon om det rettslige grunnlaget og formålet med behandlingen. <u>Gjenbruk</u> • Den registrerte får ikke tilstrekkelig informasjon om hvordan personopplysninger gjenbrukes og til hvilket formål. <u>Utlevering</u> • Det er ikke gitt informasjon om utlevering/overlevering av personopplysninger til tredjeparter eller eventuell overføring til utlandet. <u>Automatiserte avgjørelser</u> • Det er ikke gitt informasjon om at det utføres automatiserte avgjørelser som berører den registrerte.
Den registrete får ikke innsyn i all sine personopplysninger.	Innsynsbegjæring fra den registrerte blir ikke fulgt opp og tatt til følge. Det er ikke mulig å gi innsyn i opplysningene verken automatisk eller manuelt.	• Den registrerte får ikke den informasjonen vedkommende har krav å ved begjæring om innsyn.
Rettferdig		
Måten vi behandler personopplysninger på kan gi forskjellsbehandling av ellers like tilfeller	Behandlingen av personopplysninger skal gjøres i respekt for de registrertes interesser og rimelige forventninger.	• Bruk av automatiserte avgjørelser fører til forskjellsbehandling av ellers like tilfeller. • Det gjennomføres ikke tester for å sørge for at de automatisert avgjørelsene er rettferdige, ikke diskriminerende og ikke medfører urimelig resultat.
Formålsbegrensning		
Personopplysningene behandles ikke i tråd med formålet de ble innsamlet for.	Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål. Det betyr at ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist.	• Formålet er ikke fastsatt i tilstrekkelig grad ved oppstart. • Personopplysningene brukes til et annet formål enn de ble innsamlet for.

Dataminimering		
Det behandles flere personopplysninger enn det som er nødvendig for å oppnå formålet.	Ved behandling av personopplysninger skal vi begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen. Over-skuddsinformasjon skal unngås. Det må vurderes konkret om formålet med behandlingen kan oppnås med innsamling av færre, mindre detaljerte personopplysninger, uten behandling av særlige kategorier av personopplysninger eller ved bruk av anonymiserte eller pseudonymiserte data.	• Det behandles flere personopplysninger fra den registrerte enn det som er nødvendig for formålet. • Det samles inn flere personopplysninger fra tredjepart enn det som er nødvendig for formålet. • Det samles inn personopplysninger om tredjepersoner som saksbehandlingen ikke angår. <u>Gjenbruk</u> • Det gjenbrukes flere opplysninger enn det som er nødvendig. <u>Utlevering</u> • Det utleveres flere personopplysninger enn det som er nødvendig for formålet med utleveringen. <u>Statistikk og analyse</u> • Det behandles flere personopplysninger enn det som er nødvendig for statistikk- og analyseformål • Det benyttes identifiserbare personopplysninger når det vil være tilstrekkelig med avidentifiserte eller pesudonymiserte opplysninger.
Riktighet		
Person-opplysningene som behandles er ikke korrekte eller oppdaterte.	Personopplysninger må være relevante, korrekte og fullstendige ut fra formål de skal benyttes til. Dette innebærer at opplysninger som behandles skal være oppdaterte og nøyaktige, og ikke inneholde irrelevant informasjon. Opplysninger som er lagret i et register brukes ofte som grunnlag til å fatte beslutninger om de registrerte. Dette prinsippet sikrer at beslutningene ikke blir fattet på et ufullstendig eller feilaktig grunnlag.	• Opplysningene som benyttes er ikke oppdaterte fordi de hentes fra en utdatert kilde. • Den registrerte får ikke korrigert eller slettet sine personopplysninger. • Rettede/slettede opplysninger blir ikke oppdatert i alle systemer/lagringssteder. • Det er ikke iverksatt tilstrekkelige tekniske og organisatoriske tiltak for å oppdage feilaktige personopplysninger og for å sørge for at personopplysningene er oppdaterte.

Lagringsbegrensning		
Personopplysningene lagres lengre enn det som er nødvendig for formålet.	Prinsippet om lagringsbegrensning innebærer at personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.	• Det er ikke fastsatt lagringstid for de aktuelle personopplysningene, eller opplysningene lagres utover fastsatt lagringstid. • Sletteregleneomfatter ikke alle delprosesser i behandlingen, som mellomlagring og kopier av informasjonen. Rutiner for sletting av personopplysninger er ikke utarbeidet eller blir ikke fulgt.
Ansvarlighet		
Det er ikke iverksatt tilstrekkelig tiltak for å sørge for etterlevelse av personvernregelverket.	Virksomheten må kunne dokumentere at den har gjennomført tiltak for å etterleve personvern-forordningen. Virksomheten må opptre proaktivt og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid.	• Retningslinjer og rutiner for å ivareta personvern er ikke godt nok dokumentert, eller har ikke et innhold som sikrer ivaretakelse av personvern og sikkerhet i tilstrekkelig grad. • Det er uavklarte rolle- og ansvarsforhold for ivaretakelse av personvern for behandlingen som gir risiko for at oppfølging av tiltak faller mellom to stoler.

Vedlegg 5. Sjekkliste for databehandleravtaler

Inneholder avtalen følgende punkter?		Ja	Nei
1	Overordnet erklæring om overholdelse av personvernforordningen?		
2	Beskrivelse av planlagt varighet av behandlingen? Det må enten fremkomme av selve databehandleravtalen eller gjennom henvisning til en hovedavtale som regulerer dette. Vil enten være en bestemt tidsramme, for eksempel «2 år» eller beskrivelse av hvor lang oppsigelsestiden er, for eksempel «3 måneders gjensidig oppsigelsestid.»		
3	Beskrivelse av aktuell behandling og formålet med behandlingen? Det er viktig å gi beskrivelser som angir formål, beskriver kontekst m.v. Dette for å skape forståelse for helheten, rammene og hensikten med behandlingen. Særlig for en leverandør som bare bistår i deler av verdikjeden, kan det være nyttig at beskrivelsen også viser leverandøren(e)s rolle i verdikjeden.		
4	Angivelse av type personopplysninger og kategorier av registrerte som behandles? Det er særlig viktig med angivelse av opplysningenes karakter om behandlingen omfatter særlige kategorier av personopplysninger da dette er opplysninger som typisk vil trenge andre eller høyere nivå på beskyttelsestiltak. Kategorier av registrerte vil typisk være ansatte, innleide konsulenter, kunder mv.		
5	Angivelse av den behandlingsansvarliges rettigheter og forpliktelser? Selv om behandlingsansvarlig og databehandler etter loven har hver sine plikter - skal også databehandler bistå den behandlingsansvarlige med dennes plikter på en rekke områder. Det kan derfor være opplysende at det sies noe om dette, satt i kontekst med det avtalen gjelder.		
6	Presisering av at databehandler bare kan behandle personopplysningene i tråd med behandlingsansvarliges dokumenterte instruksjoner? Dette er en absolutt ramme for hva en databehandler kan foreta seg. For å forebygge misforståelser må dette presiseres i avtalen og det må beskrives hva dette innebærer i praksis.		
7	At databehandler forplikter seg til å sikre at de ansatte kun vil behandle personopplysninger i tråd med angitte konfidensialitetskrav? Det er viktig å presisere samt å sette ord på hva det betyr i praksis. Krav på dette punktet må ses i sammenheng med hvilken type informasjon det er tale om, og hvilket beskyttelsesbehov slik informasjon har.		
8	At databehandler garanterer at nødvendige tekniske og organisatoriske tiltak for å sikre tilfredsstillende informasjonssikkerhet er ivaretatt? Krav til tiltak bør være spesifisert og stå i forhold til de aktuelle informasjonsverdiers beskyttelsesbehov. Både angivelse av krav i avtalen og hvilke tiltak databehandler samlet sett iverksetter, bør være basert på risikovurderinger.		
9	At databehandler forplikter seg til ikke å benytte underleverandører uten at dette er uttrykkelig godkjent av den behandlingsansvarlige? Dette følger også uttrykkelig av loven, men kan med fordel også beskrives uttrykkelig i avtalen for å sikre bevissthet rundt dette. Se også neste punkt.		

Inneholder avtalen følgende punkter?		Ja	Nei
10	At databehandler forplikter seg til å varsle om det er aktuelt å skifte ut en godkjent underleverandør? Dette for å gi den behandlingsansvarlige tilstrekkelig med tid til å vurdere om det er ønskelig sett fra den behandlingsansvarliges side. Bestemmelser om dette bør i tillegg regulere prosedyre for varsling mv for slike tilfeller.		
11	At databehandler er ansvarlig for alle behandlinger som utføres av underleverandøren der slik bruk tillates og forsikrer om at dette vil bli ivaretatt? Dette for å sikre at kravene er stillet i hele verdikjeden og at den behandlingsansvarlige ikke stilles dårligere i tilfeller der det tillates bruk av underleverandører.		
12	At databehandler vil bistå den behandlingsansvarlige i å iverksette passende tekniske og organisatoriske tiltak, for å ivareta den behandlingsansvarliges forpliktelser? Se også punkt over om krav basert på risikovurderinger.		
13	At databehandler vil bistå i å sikre tilfredsstillende etterlevelse av kravene til sikkerhet ved behandlingen (art 32), vurdering av personvernkonsekvenser (art. 35) og forhåndsdrøfting med Datatilsynet ved høy risiko (art. 36)?		
14	At personopplysninger etter opphør av avtalen enten sletter eller leverer tilbake alle forekomster av personopplysninger - med mindre det foreligger et lovkrav om fortsatt oppbevaring hos databehandler fortsatt? Dette er viktig for å forebygge at det ligger igjen informasjon hos databehandler etter opphør av avtalen.		
15	At databehandler vil varsle den behandlingsansvarlige om instrukser innebærer brudd på forordningens eller andre rettslige rammer?		
16	At databehandler vil gjøre tilgjengelig dokumentasjon som er nødvendig for å dokumentere etterlevelse av kravene, inkludert oversikt over alle kategorier av behandlinger mv? Det er den behandlingsansvarliges plikt til å påse at alle krav er ivaretatt. Det kan både være aktuelt å dokumentere overfor kunder og tilsynsmyndigheter at alle krav er ivaretatt, men også som ledd i eget arbeid med internkontroll. Se også punkt 17 under.		
17	At databehandler bekrefter at behandlingsansvarlig kan utføre revisjoner, inspeksjoner enten selv eller ved bruk av tredjepart samt bistå ved slike revisjoner/inspeksjoner? Slik gjennomgang kan både være aktuelt som rutinemessig gjennomgang periodisk og som oppfølging av hendelser.		

Energi Norge

Hele Norge på strøm

2020