2 Krav

Sjekklisten er dynamisk, ikke uttømmende og skal oppdateres regelmessig. Dersom du har innspill til noen av punktene, vil vi gjerne høre fra deg.

Kravene til programvare, produkt, applikasjon, system, løsning eller tjeneste skal

- bidra til at personvernprinsippene blir oppfylt
- ivareta de registrertes rettigheter
- ivareta virksomhetens plikter
- sørge for at det mest personvernvennlige alternativet er standard
- sørge for at sluttproduktet er robust, sikkert og personvernvennlig

Hva må gjøres før kravene settes?

- Kartlegg behandlingen som skal gjøres og få oversikt over personopplysningene:
  - Vil det behandles personopplysninger i programvaren?
  - Avklar hvem som er behandlingsansvarlig, og eventuelle databehandlere og underleverandører. Det må inngås databehandleravtaler, og underleverandører skal godkjennes av behandlingsansvarlig.
  - Hvilket rettslig grunnlag finnes for behandlingen?
  - Hva er formålet med behandlingen?
  - Kartlegg hvilke typer personopplysninger som er *nødvendig* å behandle for å oppnå formålet. Behandling av særlige kategorier av personopplysninger og personopplysninger om straffedommer og lovovertredelser (sensitive personopplysninger) er som hovedregel forbudt, og det må avklares om ett av unntakene gjelder. Kartlegg omfanget av opplysninger i programvaren.
  - Skal personopplysninger overføres til en tredjestat eller en internasjonal organisasjon? Det stilles krav ved overføring av personopplysninger til en tredjestat eller internasjonal organisasjon. Dette inkluderer blant annet tilganger, drift og lagring. Dersom personopplysninger skal overføres til en tredjestat eller en internasjonal organisasjon må dere sikre at man har lov til å gjøre det.
  - Hvilken kontekst vil behandlingen gjøres i? Er det sannsynlig at programvaren kan bli brukt i en annen sammenheng?
- Kartlegg hvilke krav som gjelder for din virksomhet:
  - Finnes det bransje- eller adferdsnormer for bransjen eller sektoren?
  - Finnes det retningslinjer og krav der som kan hjelpe med å sette krav til programvaren?
  - Finnes det sertifiseringsordninger dere kan og bør ta sikte på å følge? Hvilke krav settes der?
  - Har Datatilsynet fattet vedtak på dette området enten mot egen virksomhet eller andre tilsvarende virksomheter som bør innføres som krav i programvaren?

Personvern- og sikkerhetskrav

- Dersom programvaren fungerer etter formålet uten identifiserbare opplysninger, skal det ikke innhentes identifiserende opplysninger.
- Personvern kan bygges inn ved bruk av pseudonymiseringsteknikker i programvaren.
- Unødig identifisering og overflødige personopplysninger innebærer større risiko for brukeren eller den som er registrert i programvaren. Det gjør dessuten programvaren mer sårbar og mer attraktiv for aktører som vil gjenbruke personopplysninger til nye formål.
- Programvaren skal kun bruke personopplysningene slik det er planlagt, og opplysningene skal slettes når det ikke er nødvendig å lagre dem lenger.
- Personopplysninger må være tilgjengelig for de som er autorisert til å bruke dem når det er nødvendig.
- Programvaren må utvikles slik at personvernet ivaretas i standardinnstillinger.
- Programvaren skal lede brukeren til den mest personvernvennlige bruksmåten. For eksempel bør deling av lokasjon være avslått som standard slik at brukeren selv kan velge å slå den på ved behov.

Krav for å dekke personvernprinsippene

Grunnleggende krav til programvaren som skal behandle personopplysninger er

- lovlighet, rettferdighet og gjennomsiktighet/åpenhet
  - Programvarens bruk av personopplysninger skal være basert på en eller flere av disse:
    - samtykke fra den registrerte
    - en avtale eller kontrakt med den registrerte
    - en rettslig forpliktelse
    - behandlingen er nødvendig for å kunne beskytte vitale interesser hos den registrerte
    - behandlingen er nødvendig for å utøve en oppgave for allmennhetens interesse eller offentlig myndighetsutøvelse
    - behandlingen er nødvendig for å forfølge rettmessige interesser (interesseavveining)
  - Programvaren skal sørge for å ivareta den registrertes rettigheter og friheter etter personvernregelverket.
  - Behandling av personopplysninger skal være forutsigbar for den registrerte og gjøres i respekt for de registrertes interesser.
  - Programvaren bør utformes slik at alle sider ved behandlingen av personopplysninger er kjent for den registrerte slik at vedkommende skal kunne ta informerte valg eller utøve sine rettigheter.
  - Programvaren skal sørge for å ivareta andre rettigheter, som for eksempel ytringsfrihet, tankefrihet og religionsfrihet.
  - Det skal gis tydelig og forståelig informasjon til den registrerte om formål for og behandling av personopplysninger.
- formålsbegrensning
  - Programvaren skal kun samle inn personopplysninger for bestemte, uttrykkelig angitte og rettmessige formål.
  - Opplysningene skal ikke behandles for andre formål som er uforenlige med opprinnelig formål.
- dataminimering

    - Programvaren skal kun behandle personopplysninger som er hensiktsmessige, relevante og begrenset til det som er nødvendig for formålet.
- riktighet
    - Programvaren skal sørge for at personopplysninger er korrekte og oppdaterte, uriktige opplysninger skal slettes eller rettes.
- lagringsbegrensning
    - Programvaren skal sørge for at det ikke er mulig å identifisere den registrerte lengre enn det som er nødvendig for formålet
- integritet og fortrolighet
    - Programvaren skal ivareta sikkerheten til personopplysningene

Dersom programvaren baserer seg på **samtykke**:

- Samtykket skal være uttrykkelig (ikke passivt), frivillig (ingen tvang/press) og informert (forutsigbart).
- En samtykkeerklæring skal skrives i et klart og enkelt språk på leserens nivå, være forståelig og være lett tilgjengelig for brukeren. Det er egne vilkår for barns bruk av informasjonssamfunnstjenester.
- Brukeren skal kunne trekke tilbake samtykket like enkelt som det er å gi samtykke.

Krav for å ivareta de registrertes rettigheter

Plikten til å gi informasjon er ulik om personopplysningene innhentes fra den registrerte eller om personopplysningene innhentes fra andre enn den registrerte.

- Når personopplysningene innhentes fra den registrerte skal det informeres om følgende:
    - hvem som er behandlingsansvarlig (identitet og kontaktinformasjon)
    - hvem som er personvernrådgiver (der det er relevant)
    - hvorfor personopplysninger behandles (til hvilket formål)
    - hva som er det rettslige grunnlaget for behandlingen (samtykke, avtale, etc)
    - hva som er de rettmessige interessene, hvis rettslig grunnlag er interesseavveining
    - hvem opplysningene deles med (mottakere), inkludert databehandlere
    - hvorvidt opplysningene skal overføres til stat utenfor EU/EØS

- Når det er nødvendig for å sikre en rettferdig og åpen behandling, skal den registrerte ha informasjon om:
    - hvor lenge personopplysningene blir lagret
    - hvordan brukere kan utøve sine rettigheter (for eksempel trekke samtykke, rette og slette data, retten til dataportabilitet)
    - behandlingen av personopplysninger skjer som følge av lovkrav, avtalefestede krav eller er nødvendig for å inngå kontrakt
    - bruk av programvaren medfører automatiserte beslutninger eller profilering, og i så tilfelle informasjon om algoritmene og betydningen/konsekvensene av slik behandling
    - det er planlagt å bruke personopplysningene til andre formål enn det de er innsamlet for, og eventuelt hvilke regler og rettigheter som gjelder med hensyn til slik behandling.

- Når personopplysningene innhentes fra andre enn den registrerte skal det informeres om
    - hvilke kategorier av personopplysninger som behandles
    - fra hvilken kilde personopplysningene stammer fra

Programvaren må gjøre det enkelt for brukeren å ivareta sine rettigheter, slik som

- rett til innsyn i egne personopplysninger, informasjon om behandlingen og andre rettigheter
- rett til korrigering av egne personopplysninger så raskt som mulig
- rett til sletting («rett til å bli glemt») av egne personopplysninger så raskt som mulig, dersom forutsetningene for sletting gjelder
- rett til å begrense behandling av egne personopplysninger, dersom forutsetningene for begrensning gjelder
- rett til dataportabilitet for egne personopplysninger, dersom behandlingen er basert på samtykke eller avtale og behandlingen utføres automatisk
- retten til å protestere mot behandling av egne personopplysninger, dersom forutsetningene for innsigelsesrett gjelder
- rettigheter ved automatiserte individuelle avgjørelser, inkludert profilering som har rettsvirkning for eller på tilsvarende måte kan ha stor betydning for vedkommende

Dersom brukeren har krevd at personopplysninger blir korrigert, slettet eller begrenset, må behandlingsansvarlig informere andre som har mottatt personopplysningene om denne korrigeringen.

Programvaren skal pseudonymisere eller anonymisere personopplysninger når det ikke lenger er behov for å ha identifiserende personopplysninger.

Programvaren skal inneholde sperrer mot kobling av personopplysninger om den registrerte til andre personopplysninger i andre system eller personopplysninger som er samlet inn til andre formål.

Krav for å ivareta virksomhetens plikter
Ved bruk av databehandlere:

- Behandlingsansvarlig skal bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre tiltak som sikrer at behandlingen etterlever personvernregelverket.
- Behandlingsansvarlig skal sikre at eventuelle leverandører og underleverandører oppfyller kravene gjennom å inngå databehandleravtaler.

For å ivareta sikkerheten til personopplysninger, må man

- sikre **konfidensialitet (K)**. Personopplysninger sikres mot uautorisert utlevering og tilgang.
- sikre **integritet (I)**. Personopplysninger sikres mot utilsiktet og ulovlig ødeleggelse, tap og endringer.
- sikre **tilgjengelighet (T)**. Personopplysninger skal være tilgjengelig for autoriserte med tjenestlig behov.

I tillegg stilles det krav i personvernregelverket om sikring av robusthet (R) og vi anbefaler også å sikre sporing (S):

- Robusthet betyr at programvare som behandler personopplysninger, skal være robuste mot for eksempel sårbarheter, angrep, og uhell.
- Sporing er dokumentering av endringer som gjøres i programvaren og på personopplysningene. Sporing har som formål å kunne håndtere sikkerhetsbrudd.

OWASP Application Security Verification Standard (ASVS) inneholder en rekke sikkerhetskrav som kan tas i bruk ved utvikling av programvare, i likhet med flere sikkerhetsstandarder. Vi gjentar dem ikke her, men anbefaler alle å vurdere hvilket nivå av sikkerhet som er tilfredsstillende for programvaren og programvareutviklingen. Vi anbefaler også å ta i bruk kravene etter tilsvarende nivå i OWASP ASVS.

Norge har flere regelverk som stiller krav til sikkerhet innenfor ulike sektorer. Hver enkelt virksomhet må sørge for å vite hvilke regler den må etterleve ved utvikling av programvare.

Nedenfor lister vi opp en rekke sikkerhetskrav som kan tas i bruk og gir eksempler på hvilke sikkerhetsaspekt som sikres (K, I, T, R, S).

- Tilgangsstyring:
  - Programvaren har tilgangsstyring (autorisasjon, autentisering og sporbarhet):
    - Brukere skal identifiseres. (S)
    - Hvilke roller skal ha hvilke rettigheter (tjenstlig behov). (T)
    - Det er mulig å kontrollere sporbarhet ved gjennomgang av logger. (S)
  - Brukere får tilgang kun til informasjon som er nødvendig for å utføre den enkeltes oppgave (tjenstlig behov). (K, T)
  - Administratorrettigheter gis til et fåtall med tjenstlig behov. (K, I, T, R, S)
  - De registrerte får tilgang til sine personopplysninger. (I, T)
  - Passord håndteres på en sikker måte og programvaren stiller krav til sterke passord. (K, I, R)
  - Programvaren støtter og krever sterk autentisering (for eksempel tofaktor-autentisering) der det er nødvendig (for eksempel kan brukere oppfordres til å ta det i bruk, mens det skal kreves av administratorer og brukere med tilgang til beskyttelsesverdige opplysninger eller opplysninger om mange). (K, I, S)
  - Programvaren må overvåke om og når noen prøver å få uautorisert tilgang. (K, I, R, S)
  - Programvaren må begrense tilgang fra tredjeparter og begrense hva en tredjepart får tilgang til (for eksempel begrense tilgang til spesifiserte IP-adresser eller gi midlertidig og begrenset tilgang). (K, I, R)
- Programvaren må sørge for å ha hensiktsmessig og tilfredsstillende informasjonssikkerhet under lagring og ved kommunikasjon av data. Kryptering kan bidra til å oppfylle dette. Ved bruk av kryptering skal det til enhver tid brukes utbredte og anerkjente algoritmer og metoder, med en nøkkellengde som er tilstrekkelig. Det må fastsettes minimumskrav til forvaltning og avklares hvor ofte sikkerhetsalgoritmer skal gjennomgås og oppdateres
  - på endepunkter (PC, laptop, telefon, nettbrett) (K, R)
  - ved fjerntilgang (K, R)
  - ved overføring og lagring i skytjenester (K, R)
  - av backup og sikkerhetskopier, og enheter som inneholder backup (K, T, R)
- Programvaren må beskytte integriteten av data og kunne å oppdage endringer i filer, servere og nettverk ved å (I)
  - sammenligne hashverdier og sjekksummer
  - begrense skrivetilgang
  - ta jevnlige integritetssjekker
  - sette referanseverdier (min/max)
- Programvaren må sikre at personopplysninger er tilgjengelig når det er nødvendig gjennom (T)
  - redundans
  - beredskapsplaner
  - hendelseshåndtering
  - programvaren må være i stand til å gjenopprette tilgjengelighet og tilgang til personopplysninger etter en hendelse
- Programvaren må være robust ved at (R)
  - den må sikres mot kjente sikkerhetshull og sårbarheter

    - den må konfigureres riktig
    - den må legge opp til segmentering av lagrede data, system, prosesser og nettverk
    - den må sørge for å oppdatere og patche programvare fra tredjeparter
    - den må ha en mulighet for å motta varsler fra brukere og andre om sårbarheter i programvaren, og sørge for at de blir håndtert og tatt seriøst
    - det sørges for sikker destruering av medier som håndterer personopplysninger
- Det stilles krav til at programvaren skal gjøre det mulig å spore endringer som gjøres og for å kunne håndtere sikkerhetsbrudd gjennom (S)
    - dokumentasjon på programvare og prosedyrer
    - logging av konfigurasjonsendringer, prosesser, aktiviteter og hendelser
    - tilgangsstyring til logger, kun for de med tjenstlig behov og når det er nødvendig at de skal ha tilgang
    - sletting eller anonymisering av logger etter en gitt frist
    - å ikke lagre logger lenger enn nødvendig

Toleransenivå for personvern og informasjonssikkerhet

- Utarbeid toleransenivå for personvern og for informasjonssikkerhet. Målet med å sette toleransenivå er å definere akseptabel risiko for sikkerhet og personvern i programvaren. Disse må baseres på etablerte og aksepterte hjelpetabeller og toleransegrenser.
- Definer toleransenivå enkeltvis for personvern og for informasjonssikkerhet. Metodikk kan gjenbrukes.
- Hjelpetabeller kan kategorisere kritikalitet som for eksempel Kritisk, Høy, Moderat og Lav. Sett inn variabler for hver kategori og avklar toleransenivået.

  Eksempler på kategorier som må ha akseptabelt toleransenivå for personvern:
    - Den registrerte skal ha kontroll på sine personopplysninger.
    - Den registrerte skal ikke miste sine rettigheter og friheter.
    - Den registrerte skal ikke diskrimineres / profileres.
    - Den registrerte skal ikke kunne utsettes for identitetstyveri eller bedrageri.
    - Den registrerte skal ikke kunne lide økonomisk tap.
    - Den registrerte skal ikke kunne lide omdømmetap.
    - Ved pseudonymisering skal man ikke uautorisert kunne spore tilbake til opprinnelig identitet.
    - Konfidensialitetsbrudd på taushetsbelagte opplysninger skal ikke forekomme.

  Eksempler på kategorier som må ha akseptabelt toleransenivå for sikkerhet:
    - Det skal ikke forekomme utilsiktet eller ulovlig ødeleggelse, tap, endring av personopplysninger.
    - Det skal ikke forekomme uautorisert utlevering eller tilgang til personopplysninger.
    - Personopplysninger skal sikres med hensyn til konfidensialitet, integritet, tilgjengelighet og robusthet i programvaren.
    - Personopplysninger skal pseudonymiseres så snart det er mulig og krypteres.
    - Det skal gjenopprettes tilgjengelighet og tilganger til personopplysninger etter fysiske og tekniske hendelser.
    - Det skal finnes prosedyrer for å regelmessig teste, vurdere og evaluere tiltakene for å se om de er tilstrekkelige for å sikre behandlingen.

Eksempel
Virksomhetens ledelse har satt toleransenivå for kategori «Skade på liv og helse» til kritikalitet Lav. Rød tekst (se tabell under) er utenfor virksomhetens toleransegrense. Dersom informasjon kompromitteres, det er mangler ved informasjonens integritet eller mangel på tilgjengelighet til informasjon medfører «Middels», «Høy» eller «Kritisk kritikalitet», er det uakseptabelt for virksomhetens ledelse. Det medfører iverksettelse av tiltak. Manglende integritet av informasjon som kan medføre «Høy kritikalitet», kan for eksempel være at det gis feil informasjon om bremser på en bil eller feil opplysning om blodtypen til en person.

Nivå kritikalitet	**Kategori – eksempel:** Skade på liv og helse
Kritisk	Dødsfall
Høy	Personskade som medfører varig uførhet
Middels	Personskade medfører sykemelding
Lav	Ingen alvorlig personskade eller sykefravær

Microsoft SDL og ISO 27034-x gir også eksempler på hvordan man kan finne toleransenivå.

Vurdering av personvernkonsekvenser og sikkerhetsrisiko

Resultatet av vurderingen skal sikre at programvaren i minst mulig grad innskrenker den registrertes personvern, at den sikrer borgerens grunnleggende rettigheter og friheter, og at den sikrer borgerens rett til vern av personopplysninger.

- Gjennomfør en vurdering av personvernkonsekvenser dersom behandlingen av personopplysninger
  - brukes til automatiserte avgjørelser og er en systematisk og omfattende vurdering av personlige forhold.
  - er behandling av sensitive personopplysninger i stort omfang.
  - er systematisk overvåking av offentlig område i stort omfang.

  Hvis dere er i tvil om plikten til å vurdere personvernkonsekvenser gjelder, anbefaler vi dere å gjøre en slik vurdering.

- En vurdering av personvernkonsekvenser skal som et minimum inneholde
  - en systematisk beskrivelse av behandlingen, formål, og eventuelt hvilken berettiget interesse den ivaretar
  - en vurdering av nødvendighet og forholdsmessighet, sett opp mot formålet
  - en vurdering av hvor stor risikoen er for de registrertes rettigheter og frihet
  - tiltak som skal iverksettes for å redusere risikoen

- Når risiko for personvernkonsekvenser er høy, skal sårbarhetsreduserende tiltak implementeres. Dette reduserer vanligvis risikoen. I tilfeller der risiko for

personvernkonsekvenser er høy og ikke kan reduseres, skal dere kontakte Datatilsynet for en forhåndsdrøftelse.

- Gjennomfør en teknisk risikovurdering av informasjonssikkerheten ved programvaren:
  - En slik vurdering skal avdekke sårbarheter og mangler ved sikkerheten i programvaren og dermed bidra til å stille tilstrekkelig sikkerhetskrav.
  - Sørg for å måle hvordan sikkerhetstiltakene fungerer.
  - Ta gjerne utgangspunkt i standarder og og eksempler på hvordan gjennomføre riskokoanalyse, for eksempel ISO27005, Datatilsynets veileder om risikovurdering og Difi sin veiledning for internkontroll og informasjonssikkerhet.