Personvern i Norges Sildesalgslag

Innhold

1. Om personverndokumentet

Dette dokumentet skal bidra til at Norges Sildesalgslag (NSS) etterlever lov om personopplysninger fra 2018. Dokumentet skal også bidra til å påvise at NSS sin behandling av personopplysninger er i samsvar med loven.

2. Ansvar for behandling av personopplysninger i NSS

NSS er ansvarlig for personopplysninger som behandles, for eksempel om egne ansatte, fiskere og kjøpere, kontaktpersoner hos kunder og leverandører, medlemmer, tillitsvalgte og andre forretningsforbindelser. NSS har ansvaret for å overholde de pliktene som følger av reglene om personopplysninger.

Det daglige behandlingsansvaret i NSS har daglig leder

3. Kunnskap om reglene om personopplysninger

NSS skal sørge for at de relevante ansatte har kjennskap til reglene om personopplysninger, herunder dette dokumentet om personvern. Kunnskapsnivået skal være tilpasset den enkelte ansattes behandling av personopplysninger. NSS skal vurdere om noen grupper av ansatte har behov for særlig kunnskap, for eksempel personalfunksjoner og IT-ansvarlige. Ledelsen i NSS skal alltid ha kjennskap til regelverket.

4. Kartlegging av behandling av personopplysninger

NSS skal kartlegge all behandling av personopplysninger. Dette skal gjøres i et egne rutiner der det angis blant annet kategorier av registrerte, formål med behandlingen, hvordan behandles opplysningene og hvilke grunnlag som finnes for behandlingen. Rutinene skal bidra til at NSS etterlever reglene om behandling av personopplysninger.

5. Grunnkrav for behandling av personopplysninger

Loven stiller opp seks grunnkrav som gjelder for all behandling av alle personopplysninger. NSS skal sørge for at personopplysninger skal:

1) behandles på en lovlig, rettferdig og gjennomsiktig måte med hensyn til den registrerte («lovlighet, rettferdighet og gjennomsiktighet»)

2) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene («formålsbegrensning»)

3) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»)

4) være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller korrigeres («riktighet»)

5) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for («lagringsbegrensning»)

6) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og fortrolighet»)

Hvis personopplysninger brukes til andre formål enn de er samlet inn for, se punkt 2 ovenfor, skal NSS alltid vurdere om nye eller endrede formål er forenlig med det opprinnelige. Vi skal da ta hensyn til de faktorene som fremgår av personvernforordningen artikkel 6 nr. 4.

6. Grunnlag for å behandle personopplysninger

6.1. Behandlingsgrunnlag

Vi skal ha minst ett av følgende grunnlag for all behandling av personopplysninger:

1) den registrerte har gitt samtykke til behandling av sine personopplysninger for ett eller flere spesifikke formål

2) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse

3) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige

4) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn (interesseavveining)

Det skal gå frem av rutinen hvilke(t) grunnlag som finnes for å behandle opplysninger.

Hvis grunnlaget for behandling er samtykke fra den registrerte (se nr. 1), skal vi sette oss inn i de særlige reglene som gjelder for slike samtykker, blant annet kravet om dokumentasjon.

Hvis grunnlaget for behandling er vår berettigede interesse (interesseavveining) (se nr. 4), skal vi konkret og skriftlig dokumentere avveiningen, se nærmere nedenfor.

6.2. Ansatte

Behandling av opplysninger er i hovedsak rettslige forpliktelser. Noe av behandlingen er basert også på interesseavveining. Det er behov for å dokumentere at forpliktelser etter lov og avtale er oppfylt. Det er også behov for dokumentasjon av personaladministrasjon til bruk for fremtidig personaladministrasjon. Dette er berettigede interesser. Det er ikke mulig å ha tilgang til opplysningene på annen måte enn å lagre opplysningene. Behandling er derfor nødvendig.

Ansatte i Norges Sildesalgslag har et løpende avtaleforhold med bedriften. Personopplysningene NSS behandler er knyttet til dette avtaleforholdet. Det er i stor grad snakk om opplysninger ansatte har gitt. Opplysningene gjelder forhold det er nærliggende at en arbeidsgiver behandler.

NSS mener at den berettigede interessen går foran den ansattes interesser.

6.3. Tidligere ansatte

Behandlingen av de fleste av personopplysningene er basert på interesseavveining. Det kan oppstå behov for å dokumentere personalforhold også etter at arbeidsforholdet er avsluttet, for eksempel ved en tvist med den tidligere ansatte. Dette kan gjelde for eksempel dokumentasjon for at NSS har oppfylt sine forpliktelser etter lovgivning eller arbeidsavtale. Dette er en berettiget interesse. Det er ikke mulig å ha tilgang til opplysningene på annen måte. Behandling er derfor nødvendig.

Behandlingen går ut på å lagre opplysningene i opptil 3 år. Opplysninger om at den ansatte har vært ansatt, varighet av arbeidsforholdet og arbeidsoppgaver kan lagres lenger. Opplysningene vil ikke bli utlevert til andre uten at den tidligere ansatte ber om det, for eksempel i forbindelse med vurdering av ansettelse hos ny arbeidsgiver.

NSS mener at den berettigede interessen går foran den tidligere ansattes interesser.

6.4. Jobbsøkere

Behandlingen av personopplysninger er basert på interesseavveining. Bedriften har behov for å bruke opplysninger for å vurdere søknader jobbsøkere sender oss. Dette er en berettiget interesse. Det er ikke mulig å vurdere en søknad uten å behandle personopplysninger. Behandling er derfor nødvendig.

NSS ber de som vil søke jobb i bedriften om å sende oss minst opplysninger om navn, utdanning, arbeidserfaring, referansepersoner mv (CV). Jobbsøkere vil ofte gi ytterligere personopplysninger de regner som relevante for vurderingen av søknaden, for eksempel om kontaktinformasjon, familieforhold og interesser, i tillegg. I intervjuer stilles spørsmål for å avgjøre om jobbsøkeren passer til stillingen. I noen tilfeller brukes tester eller spørsmålsskjemaer for dette formålet. Hvis det blir aktuelt å ansette jobbsøkeren vil vi kunne be om ytterligere informasjon samt om dokumentasjon for opplysninger vi allerede har fått. Det er frivillig å gi oss opplysninger.

NSS bruker ikke opplysningene til noe annet enn å vurdere søknaden. NSS gir ikke opplysningene til noen andre. NSS kan beholde opplysninger fra jobbsøkere i ett år, i tilfelle jobbsøkere skulle mene at deres rettigheter ikke er oppfylt. Eller NSS ønsker kontakt for eventuelt andre stillinger som måtte være ledige.

NSS mener at den berettigede interessen går foran jobbsøkerens interesser.

6.5. Kontaktpersoner hos fiskere og kjøpere

NSS behandler opplysninger om kontaktpersoner hos rederier, kjøpere og mottaksanlegg som en del av vår oppgave som førstehåndsomsetter av pelagisk fisk.

Sluttsedler og landingssedler kan inneholde personopplysninger og vil da vil være en del av lovpålagt rapportering til Fiskeridirektoratet.

Grunnlaget for å behandle personopplysninger knyttet til slutt- og landingssedler er personvernforordningens artikkel 6-1 e som sier at personopplysninger kan behandles hvis det er nødvendig for å kunne utøve offentlig myndighet.

Seddeldataene inngår som en del av fiskeri- og kvotestatistikken for nasjonen Norge. Sluttsedler og landingssedler lagres derfor så lenge det er teknisk mulig.

Slutt- og landingssedler skal ifølge Landingsforskriften signeres av skipper og kjøper/mottakers representant (partene). For å kunne signere elektronisk kreves det en signeringsidentitet med fødselsdato, navn og adresse som personen selv oppgir. Denne blir lagret hos salgslagenes felles selskap Catch Certificate SA.

En slutt- eller landingsseddel som er elektronisk signert, vil i tillegg til eventuelle andre persondata inneholde:

- Partenes signaturer
- Dato/klokkeslett for signering
- Partenes geografiske posisjon ved signering

NSS kan gi innsyn i slutt- og landingssedler dersom det fremsettes et berettiget krav om dette i medhold av bestemmelser i offentlighetslova.

Fiskermanntall med personnummer som mottas elektronisk fra Fiskeridirektoratet er nødvendige opplysninger for å kunne utføre lovpålagt kontroll. Dataene benyttes kun for å sjekke manntallstatus for fartøy. Kun sist oppdaterte versjon mottatt fra Fiskeridirektoratet lagres.

Våre elektroniske registre inneholder navn og kontaktinformasjon til personer tilknyttet rederier og kjøpere. Denne informasjonen blir innhentet fra personen selv eller fra dennes arbeidsgiver. Lagring av kontaktinfo er nødvendig for å kunne utøve den daglige drift på en effektiv og god måte både ved omsetning/oppgjør og som kontrollmyndighet (berettiget interesse). Navn og kontaktinfo slettes så snart vi får kjennskap til at personen ikke lenger er tilknyttet aktuelt firma.

For å kunne tilby avtalt tilgang til vår Ekstranettside/NSS App (egne retningslinjer) er det også nødvendig å lagre kontaktinformasjon. Slik tilgang baserer seg på en avtale med personen selv eller dennes arbeidsgiver.
Navn og kontaktinfo anonymiseres eller slettes når det ikke lenger er nødvendig å ha disse. Det kan variere hvor lenge det er nødvendig å ha opplysningene.

Personopplysninger kan deles med offentlig myndighet.

6.6. Andre kontaktpersoner

Behandling av personopplysninger er basert på interesseavveining. NSS har behov for å ha kontakt med offentlige myndigheter, for eksempel NAV og tilsynsmyndigheter, revisor i forbindelse med offentligrettslige forhold der vi kan ha forpliktelser og rettigheter. Dette er en berettiget interesse. I en del tilfeller vil den kommunikasjonen kunne være effektiv bare hvis vi kan kontakte enkeltpersoner direkte. Behandling er derfor nødvendig.

NSS lagrer navn og kontaktdetaljer og bruker opplysningene til å kontakte personens arbeidsgiver. Opplysningene er knyttet til kontaktpersonens arbeidsgivers virksomhet og ikke til kontaktpersonens privatliv. NSS behandling av personopplysningene er klart påregnelig for kontaktpersonen.

NSS lagrer også kontaktinformasjon om personer hos Fiskeridirektoratet, og Kystvakten og evt. andre kontrollmyndigheter for at disse skal kunne benytte seg av lagets kontrollsider og prisinformasjon som en del av deres utøvelse av kontrollansvar som offentlig myndighet.

Lagring av navn, telefonnummer, epostadresse og stilling og avdeling baserer seg på en brukeravtale som hver enkelt person og dennes offentlige arbeidsgiver må signere for å få slik tilgang. Navn/kontaktinfo oppbevares også en viss tid etter at bruker har sluttet for å kunne vise til historikk.

NSS lagrer også kontaktinformasjon til personer hos revisor, banker, leverandører m.m. for å gjøre det enklere å kunne ringe og sende mail. Navn og kontaktinfo slettes så snart NSS får kjennskap til at personen har sluttet.

NSS mener at den berettigede interessen går foran kontaktpersonens interesser.

7. Grunnlag for behandling av sensitive personopplysninger

Behandling av sensitive personopplysninger krever behandlingsgrunnlag i tillegg til de som er nevnt i punkt 6.

Sensitive personopplysninger er: opplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap, samt 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.

NSS behandler vanligvis aldri slike opplysninger. Skal vi behandle slike opplysninger, skal det sørges for å ha behandlingsgrunnlag. For ansatte vil opplysninger om fagforeningsmedlemskap være aktuelle med bakgrunn i trekk av fagforeningskontingent over lønn. NSS vil vanligvis ikke behandle helseopplysninger bortsett fra de opplysninger som formidles via sykmelding til arbeidsgiver og oppfølging av sykmeldte etter gjeldende sykefraværsrutiner. Eller spesiell tilrettelegging med bakgrunn i helsespørsmål i arbeidsforhold i egenskap av arbeidsgiver.

Behandling av opplysninger om straffbare forhold og lovovertredelser o.l. er underlagt særlige regler som vi skal sette oss inn i hvis vi skal behandle slike opplysninger.

8. Informasjon til de registrerte (personvernerklæring)

NSS skal gi lovbestemt informasjon til de registrerte. Vi skal gi slik informasjon i en personvernerklæring. Alle registrerte skal ha tilgang til den informasjonen som gjelder dem. Informasjon til ansatte gir vi i personalhåndbok og/eller Intranett

Informasjonen skal inneholde blant annet navnet på bedriften og kontaktinformasjon, formålet med behandlingen, kategoriene av personopplysninger, mottakere av personopplysninger (dersom de utleveres), informasjon om eventuell utlevering av personopplysninger til andre land, hvor lenge personopplysningene vil bli lagret, de registrertes rett til å kreve innsyn, rette eller kreve slettet personopplysningene, hvordan virksomheten fikk tilgang til personopplysningene og muligheten til å klage virksomheten inn til Datatilsynet.

9. Registrertes rettigheter

NSS skal besvare henvendelser fra registrerte uten ugrunnet opphold. Mottar vi slike henvendelser, skal de sendes til daglig leder.

NSS skal sørge for at registrerte får gjennomført rettighetene sine hos oss.

10. Sletting av personopplysninger

NSS skal slette personopplysninger uten ugrunnet opphold når de ikke lenger er nødvendig for formålet som de ble samlet inn eller behandlet for. Minst én gang i året skal dette gjennomgås. Våre retningslinjer for sletting følger nedenfor eller av kartleggingsskjemaet.

Ansatte

NSS beholder som hovedregel alle opplysninger i hele ansettelsestiden. Ansatte kan be om at opplysninger blir slettet. Dette vil bli vurdert konkret. Lovgivningen kan stille krav til lengre oppbevaringstid.

Tidligere ansatte og jobbsøkere

Se ovenfor om behandlingsgrunnlaget for disse kategoriene. Lovgivningen kan stille krav til lengre oppbevaringstid enn det som fremgår der.

Kontaktpersoner hos kjøpere og fiskere

Kontaktpersoner hos fiskere og kjøpere blir merket med «slettet» så snart vi får kjennskap til at personen ikke lenger er ansatt i aktuelt firma. Øvrige opplysninger om vedkommende som epost og tlf.nr vil da bli slettet automatisk. Denne rutinen gjelder fra 1.1.2022.
Generelt kan kontaktinfo til personer med brukertilgang bli oppbevart en stund utover utløpstiden for brukertilgangen. Dette for å kunne tilby en bedre service i tilfeller der personen på nytt skal ha tilgang. Grunnlag er berettiget interesse.

Medlemmer

Når medlemmer melder seg ut eller på annen måte ikke lenger er medlem, eller hvis fartøyet de er registrert på ikke har levert fangst i ett av de to siste år for med enn 1G, jfr NSS vedtekter, settes medlemmet i «slettet». Det betyr at personlige opplysninger som adresse, fødselsdato, epost og tlf.nr blir da automatisk slettet. Grunnlaget er berettiget interesse for statistisk til enhver tid å ha statistikk over antall medlemmer og bevegelser innenfor medlemsmassen. Dette gjelder fra 1.1.2022.

Tillitsvalgte

Styremedlemmer og øvrige tillitsvalgte skal slettes når lovgivningen tilsier sletting mht rapportering til offentlig myndighet av lønn og honorarer. Det vil bli registrert i NSS årsmelding navn på hvem som til enhver tid har sittet i årsmøtet, styret og øvrige tillitsmannsutvalg, og hvilket distrikt og gruppe de har representert. Dette for å følge NSS vedtekter og vedlikehold av selskapets alminnelige historikk.

Andre kontaktpersoner – herav leverandører og kunder som ikke er kjøpere eller fiskere i førstehåndsomsetningen

NSS skal slette opplysningene når det blir kjent med at kontaktpersonen har sluttet hos leverandøren eller kunden eller at leverandøren eller kunden har utpekt en ny kontaktperson. Det samme gjelder når leverandør- eller kundeforholdet er opphørt.

NSS kan likevel lagre opplysningene for en lengre periode hvis vi mener det kan bli nødvendig med dokumentasjon av den kontakten vi har hatt med leverandøren eller kunden. Det kan gjelde for eksempel spørsmål om rettigheter eller forpliktelser i avtaleforholdet med leverandøren eller kunden. Også lovgivningen kan stille krav til lengre oppbevaringstid.

NSS skal slette opplysningene når det blir kjent at personen ikke lenger er relevant for våre behov, herunder hvis personen slutter hos den bedriften, offentlig etaten osv.

Opplysningene kan likevel lagres for en lengre periode hvis det kan bli nødvendig med dokumentasjon, kontakt med personen eller personens arbeidsgiver. Det kan gjelde for eksempel spørsmål om rettigheter eller forpliktelser i avtale-, offentligrettslige eller andre forhold.

11. Personvernombud

NSS har vurdert om personvernforordningen krever at vår bedrift skal ha personvernombud.

NSS har svært få fysiske personer som kunder. NSS driver ikke regelmessig og systematisk monitorering i noen skala av registrerte. For de fleste kategorier av registrerte behandles stort sett alminnelige personopplysninger som navn, adresse, arbeidsgiver, epostadresse, telefonnummer o.l. NSS behandler enkelte sensitive opplysninger om ansatte.

NSS har konkludert med at vår bedrift ikke er underlagt krav om å ha personvernombud.

12. Alminnelig risikovurdering

NSS skal risikovurdere behandlingen av personopplysninger. Denne vurderingen skal gjøre at en er i stand til å identifisere og definere hvilke sikkerhetstiltak som skal gjennomføres.

Vurderingene skal gjelde sannsynlighet og alvorlighetsgrad (risiko) for personers "rettigheter og friheter", som fysisk skade, skade på ting eller formue og medisinsk skade. Eksempler på skader er diskriminering, identitetstyveri, omdømmeskade, tap av sosial aktelse, at konfidensielle opplysninger blir kjent for uvedkommende og uakseptable inngrep i privatlivets fred.

NSS' gjennomgang viser at vi:

- i stor grad behandler bare alminnelige kontaktopplysninger, som navn, adresse, arbeidsgiver, epostadresse, telefonnummer o.l.
- behandler opplysninger om ansatte som er vanlige for å administrere personalforhold, herunder etterlevelse av lovpålagte forpliktelser
- har svært få privatkunder
- ikke behandler opplysninger om barn
- behandler opplysninger som er en del av det å drive alminnelig næringsvirksomhet

NSS er ikke kjent med at utenforstående har vist interesse for de personopplysningene selskapet behandler. Basert på arten og omfanget av de opplysningene vi behandler, mener vi at konsekvensene ved regelbrudd ikke vil være alvorlige.

Når det gjelder en del av opplysningene om ansatte er både sannsynlighet for og alvoret ved regelbrudd en del større. NSS har derfor egne rutiner for behandling av slike opplysninger, herunder begrensning av tilgang til dem.

NSS skal risikovurdere endringer som kan påvirke informasjonssikkerheten, for eksempel når vi kjøper nye IT-tjenester.

Resultatene av risikovurderinger skal godkjennes av den som har det daglige behandlingsansvaret i bedriften.

13. Informasjonssikkerhet

NSS skal etter loven treffe passende tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som svarer til risikoen knyttet til behandling av personopplysninger. NSS skal da ta hensyn til teknologi, gjennomføringskostnader og behandlingens karakter, omfang og formål, samt sammenhengen den utføres i.

Risikoen er vurdert overordnet i punktet ovenfor.

På denne bakgrunn har vi gjennomført disse tiltakene:

- Det er utpekt en person hos oss med særlig oppgave å påse sikkerheten: IT-leder
- Uvedkommende skal hindres tilgang til personopplysningene eller utstyr disse er lagret på,
- Det skal sikres at virksomhetens nettverk er beskyttet mot inntrengning fra eksterne nettverk med brannmur som kun slipper gjennom nødvendig datatrafikk,
- Det skal sikres at virksomhetens nettverk er beskyttet mot uvedkommendes bruk, eksempelvis ved sikring av trådløst nettverk.
- Ekstra tiltak er iverksatt for spesielt beskyttelsesverdige opplysninger som for eksempel opplysninger rundt tilrettelegging av arbeidsplassen, vurderinger av den ansatte, merknader og advarsler, ved at det kun er leder personal og daglig leder som øverste ansvarlige for personalarbeid, som har tilgang til disse områdene. Sykemeldinger har også lønnsansvarlige tilgang til, samt den enkeltes avdelingsleder (via Altinn).
- Ansatte skal gis opplæring i bruk av virksomhetens IT-system.

14. Avvik, analyse av avvik og tiltak for å rette opp i dem

NSS må finne ut om behandlingen av personopplysninger følger reglene i personopplysningsloven og rutinene i dette dokumentet. Er det ikke tilfellet, må det finnes ut hvordan en oppfyller etterlevelsen. Det skal dokumenteres skriftlig både hvilke avvik vi har funnet og hva som er gjort for å rette dem opp.

NSS rutiner skal kunne oppsummere avvik for hver kategori av registrerte, og avvik skal uten opphold meldes til daglig leder.

Viser det seg at rutinene ikke er godt nok tilpasset vår bedrift, må det vurderes å endre rutinene, se punkt 18.

15. Kjøp av IT-tjenester – databehandleravtaler

Vanligvis vil NSS opptre som behandlingsansvarlig når virksomheten kjøper IT-tjenester fra en tjenesteleverandør. NSS har da fortsatt ansvaret for at personvernlovgivningen blir etterlevd ved kjøp av IT-tjenester, for eksempel HR-løsninger eller kundedatabaser/CRM.

Før NSS kjøper IT-tjenester skal det derfor blant annet vurderes om leverandøren tilfredsstiller de kravene til sikkerhet som personopplysningsloven krever (artikkel 32). Seriøse leverandører vil ofte kunne dokumentere at de oppfyller kravene. NSS må sørge for å inngå en databehandleravtale som regulerer hvordan databehandleren skal håndtere personopplysningene den mottar fra og behandler på vegne av oss. Leverandører vil ofte ha egne avtaler som oppfyller kravene i regelverket.

Dersom tjenesteleverandøren skal overføre personopplysninger til land utenfor EU/EØS, må det foreligge et lovlig grunnlag for dette.

16. Brudd på personopplysningssikkerheten

Ved brudd på personopplysningssikkerheten (for eksempel hackerangrep eller tap av personopplysninger) skal NSS straks kontakte Datatilsynet for å finne ut hvilke tiltak som skal gjennomføres.

"Brudd på personopplysningssikkerheten" betyr brudd som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som vi behandler.

Ved visse brudd på personopplysningssikkerheten skal NSS varsle Datatilsynet og av og til også den registrerte. Varsling til Datatilsynet skal skje med én gang, og senest 72 timer etter at NSS ble kjent med bruddet. Det er ikke nødvendig å varsle Datatilsynet hvis det er lite trolig at bruddet på personopplysningssikkerheten vil føre med seg risiko for enkeltpersoners rettigheter. Et eksempel er der et sikkerhetsbrudd har ført til at uvedkommende har fått tilgang til personopplysninger som allerede er offentlig tilgjengelige.

NSS har plikt til å varsle den registrerte dersom det er trolig at bruddet på personopplysningssikkerheten vil medføre *høy* risiko for enkeltpersonenes rettigheter og friheter. NSS mener at vår behandling av personopplysninger bare helt unntaksvis kan føre til slik risiko.

NSS skal dokumentere eventuelle brudd på personopplysningssikkerheten. Dette gjør vi ved å beskrive de faktiske forholdene rundt bruddet ("Hva har skjedd?"). I tillegg skal virkningene av bruddet beskrives og hvilke tiltak som er truffet for å avhjelpe bruddet. Denne dokumentasjonen skal gjøre det mulig for Datatilsynet å kontrollere at virksomheten har etterlevd kravene i loven.

17. Vurdering av personvernkonsekvenser og forhåndskonsultering med Datatilsynet

NSS skal utrede personvernkonsekvensene når bedriften planlegger en behandling av personopplysninger som sannsynligvis vil utgjøre høy risiko for personers rettigheter, som retten til personvern. I vurderingen av om det er nødvendig med en slik utredning skal NSS ta hensyn til arten, omfanget, sammenhengen og formålet med behandlingen. NSS skal også ta hensyn til om bedriften benytter ny teknologi.

Det er flere typetilfeller der det er nødvendig å utrede personvernkonsekvenser: Systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser, behandling av sensitive personopplysninger i stort omfang eller systematisk overvåking av offentlig område i stort omfang.

I tilfellene ovenfor skal NSS sette seg inn i de særlige reglene som gjelder, blant annet om at Datatilsynet av og til skal involveres i forhåndsdrøftelser.

18. Kontroll, oppdatering og revisjon av dokumentet

NSS skal oppdatere og revidere dette dokumentet jevnlig og minst hvert år. Bakgrunnen er blant annet at reglene i lov og forskrift kan bli endret, NSS behandling av personopplysninger kan bli endret eller erfaringer kan tilsi at rutiner bør endres.

Det er daglig leder som har ansvar for at behov for endringer og revisjoner blir identifisert og innarbeidet i dokumentet og i skjemaet. Dette skal gjøres årlig.

Evalueringen bør omfatte for eksempel følgende spørsmål:

- Har NSS siden forrige revisjon endret (nye, endrede eller avsluttede) behandlinger av personopplysninger som ikke er behandlet i dokumentet eller i skjemaene?
- Tilsier de seks grunnkravene til behandling av personopplysninger at vi bør endre rutiner eller praksis?
- Har det siden forrige revisjon trådt i kraft nye regler i lov eller forskrift som tilsier endringer?
- Har virksomheten siden forrige revisjon oppdaget andre områder for forbedring av dokumentet eller skjemaene?
- Har det kommet ny teknologi som gjør at personopplysninger kan sikres på en bedre måte?

Bergen, 17. januar 2022

NORGES SILDESALGSLAG