Personverndokument

For Tana Arbeidsservice AS

1. OM PERSONVERNDOKUMENT
2. ANSVAR FOR BEHANDLING AV PERSONOPPLYSNINGER HOS OSS
3. KUNNSKAP OM REGLENE OM PERSONOPPLYSNINGER
4. KARTLEGGING AV BEHANDLING AV PERSONOPPLYSNINGER
5. GRUNNKRAV FOR BEHANDLING AV PERSONOPPLYSNINGER
6. GRUNNLAG FOR Å BEHANDLE PERSONOPPLYSNINGER

6.1 BEHANDLINGSGRUNNLAG

6.2 ANSATTE

6.3 TIDLIGERE ANSATTE

6.4 JOBBSØKERE

6.5 DELTAKERE PÅ ARBEIDSMARKEDSTILTAK – VTA OG AFT

6.6 KONTAKTPERSONER HOS OPPDRAGSGIVER, SAMARBEIDSPARTNERE OG LEVERANDØRER

6.7 ANDRE KONTAKTPERSONER

7. GRUNNLAG FOR BEHANDLING AV SENSITIVE PERSONOPPLYSNINGER
8. INFORMASJON TIL DE REGISTRERTE (PERSONVERNERKLÆRING)
9. REGISTRERTES RETTIGHETER
10. SLETTING AV PERSONOPPLYSNINGER
11. PERSONVERNOMBUD
12. ALMMINNELIG RISIKOVURDERING
13. INFORMASJONSIKKERHET
14. AVVIK, ANALYSE AV AVIK OG TILTAK FOR Å RETTE OPP I DEM
15. KJØP AV IT-TJENESTER – DATABEHANDLERAVTALER
16. BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN
17. VURDERING AV PERSONVERNKONSEKVENSER OG FORHÅNDSKONSULTERING MED DATATILSYNET
18. KONTROLL, OPPDATERING OG REVISJON AV DOKUMENTET

1. Om personverndokumentet

Dette dokumentet skal bidra til at vi etterlever lov om personopplysninger fra 2018. Dokumentet skal også bidra til å påvise at vår behandling av personopplysninger er i samsvar med loven.

2. Ansvar for behandling av personopplysninger hos oss

Bedriften er ansvarlig for personopplysninger vi behandler, for eksempel om egne ansatte, tiltaksdeltakere, kontaktpersoner hos kunder og leverandører, og andre forretnings-forbindelser. Bedriften har ansvaret for å overholde de pliktene som følger av reglene om personopplysninger. Det daglige behandlingsansvaret har daglig leder.

3. Kunnskap om reglene om personopplysninger

Vi 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. Vi skal vurdere om noen grupper av ansatte har behov for særlig kunnskap, for eksempel personalfunksjoner og IT-ansvarlige. Ledelsen hos oss skal alltid ha kjennskap til regelverket.

4. Kartlegging av behandling av personopplysninger

Vi skal kartlegge all behandling av personopplysninger. Dette skal gjøre vi i et eget skjema der vi angir blant annet kategorier av registrerte, formål med behandlingen, hvordan vi behandler opplysningene og hvilke grunnlag den har for behandlingen. Skjemaene skal bidra til at vi etterlever reglene om behandling av personopplysninger.

5. Grunnkrav for behandling av personopplysninger

Loven stiller opp seks grunnlag som gjelder for all behandling av alle personopplysninger. Vi 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 viderebehandle på en måte som er uforenlig med disse formålene («formålsbegrensning»)
3) være tilstrekkelige, 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 vi alltid vurdere om det nye eller endrede formålet 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 kartleggingsskjemaet hvilke(t) grunnlag vi har 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. Vi har behov for å dokumentere at vi har oppfylt forpliktelser etter lover og avtaler som gjelder ansettelsesforholdet. 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 hos oss har et løpende avtaleforhold med oss. Personopplysningene vi behandler er knyttet til dette avtaleforholdet. Det er i stor grad snakk om opplysninger ansatte har gitt oss. Opplysningene gjelder forhold det er nærliggende at en arbeidsgiver behandler. Vi 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 oss for å dokumentere personalforhold også etter at arbeidsforholdet er avsluttet, for eksempel en tvist med den tidligere ansatte. Dette kan gjelde for eksempel dokumentasjon for at vi som arbeidsgiver har oppfylt våre forpliktelser etter lovgivning eller arbeidsavtalen. 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 inntil tolv måneder. Opplysninger om at den ansatte har vært ansatt, varighet av arbeidsforholdet og arbeidsoppgaver kan vi lagre 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. Vi mener at den berettigede interessen går foran den tidligere ansattes interesser.

6.4. Jobbsøkere

Behandlingen av personopplysninger er basert på interesseavveining. Vi 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.

Vi ber de som vil søke jobb hos oss 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 stiller vi spørsmål for å avgjøre om jobbsøkeren passer til stillingen. I noen tilfeller kan vi bruke tester eller spørsmåls skjemaer 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.

Vi bruker ikke opplysningene til noe annet enn å vurdere søknaden. Vi gir ikke opplysningene til noen andre. Vi kan beholde opplysninger fra jobbsøkere i seks måneder, i tilfelle jobbsøkere skulle mene at deres rettigheter ikke er oppfylt. Vi mener at den berettigede interessen går foran jobbsøkerens interesser.

6.5. Deltakere på Arbeidsmarkedstiltak - VTA og AFT

Tana Arbeidsservice AS har inngått en skriftlig databehandler avtale med NAV. Tana Arbeidsservice AS mottar de opplysningene om deltaker som NAV mener er nødvendige ved innsøkingen til tiltaket. Deltaker skal involveres og gjøres kjent med hvilke opplysninger som sendes over og hvorfor, og at tiltaksarrangøren ivaretar opplysningene etter personvernloven. Databehandler kan ikke behandle personopplysningene på andre måter enn det som følger av avtalen med NAV.
Personopplysninger holdes isolert fra databehandlers øvrige informasjonssystem. Det er egen teknisk og fysisk løsning for personopplysningene.
Taushetsplikt
Ansatte som opptrer på databehandlers vegne blir pålagt taushetsplikt og skal undertegne på NAV sin taushetserklæring.
Alle opplysninger om en tiltaksdeltaker skal være underlagt taushetsplikt.
Taushetsplikten gjelder også etter avtalens opphør, og etter fratredelse i jobb hos databehandler.
Krav ved opphør av avtalen
Alle personopplysninger mottatt på vegne av NAV skal leveres tilbake til NAV.
Alle personopplysninger som er lagret elektronisk skal slettes.
Tana Arbeidsservice AS skal dokumentere at sletting er gjennomført.

6.6. Kontaktpersoner hos oppdragsgiver, samarbeidspartnere og leverandører

Behandlingen av personopplysninger er basert på interesseavveining. Vi har behov for å holde kontakt med oppdragsgiver, våre samarbeidspartnere og leverandører for å følge opp blant annet tilbud, bestillinger og leveranser. Dette er en berettiget interesse. Den kontakten blir effektiv bare ved å kontakte enkeltpersoner direkte. Behandling er derfor nødvendig.

Behandlingen skjer overfor kontaktpersonens arbeidsgiver, som ønsker å være leverandør hos oss. I tillegg til navn behandler vi kontaktopplysninger, som telefonnummer, e-postadresse og arbeidsgiver, som alle er knyttet først og fremst til kontaktpersonens

arbeidsforhold og ikke til kontaktpersonens privatliv. Omfanget av opplysningene er svært begrenset. Behandlingen av opplysningene er knyttet til leverandørens næringsvirksomhet og ikke til kontaktpersonens privatliv. Vår behandling av personopplysningene er klart påregnelig for kontaktpersonen.

Vi mener at den berettigede interessen går foran kontaktpersonens interesser.

6.7. Andre kontaktpersoner

Behandling av personopplysninger er basert på interesseavveining. Vi har behov for å ha kontakt med offentlige myndigheter, for eksempel NAV og tilsynsmyndigheter 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.

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

Skal vi behandle slike opplysninger, skal vi sørge for å ha behandlingsgrunnlag. For ansatte hos oss vil opplysninger om helse og fagforeningsmedlemskap være særlig aktuelle. Helse omfatter for eksempel sykdom og skader og fravær begrunnet i dette. Særlig aktuelt behandlingsgrunnlag vil være at behandling er nødvendig i egenskap av arbeidsgiver, for eksempel ved oppfølgning og rapportering til offentlige myndigheter eller ved tilrettelegging av arbeidsforholdet.

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)

Vi 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.

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.

Databehandleravtale med NAV:

Tana Arbeidsservice AS har inngått en skriftlig databehandler avtale med NAV. Tana Arbeidsservice AS mottar de opplysningene om deltaker som NAV mener er nødvendige ved innsøkingen til tiltaket. Deltaker skal involveres og gjøres kjent med hvilke opplysninger som sendes over og hvorfor, og at tiltaksarrangøren ivaretar opplysningene etter personvernloven. Databehandler kan ikke behandle personopplysningene på andre måter enn det som følger av avtalen med NAV.

Personopplysninger holdes isolert fra databehandlers øvrige informasjonssystem. Det er egen teknisk og fysisk løsning for personopplysningene.

Taushetsplikt

Ansatte som opptrer på databehandlers vegne blir pålagt taushetsplikt og skal undertegne på NAV sin taushetserklæring.

Alle opplysninger om en tiltaksdeltaker skal være underlagt taushetsplikt.

Taushetsplikten gjelder også etter avtalens opphør, og etter fratredelse i jobb hos databehandler.

Krav ved opphør av avtalen

Alle personopplysninger mottatt på vegne av NAV skal leveres tilbake til NAV.

Alle personopplysninger som er lagret elektronisk skal slettes.

Tana Arbeidsservice AS skal dokumentere at sletting er gjennomført.

(Jfr. Databehandleravtalen med NAV og Prosedyre for konfidensialitet og informasjonsbehandling av august 2018).

Hvis den registrerte er barn, skal vi vurdere særlig hvordan god informasjon kan gis.

9. Brukerens rettigheter

Vi skal besvare henvendelser fra brukerens uten ugrunnet opphold. Mottar vi slike henvendelser, skal de sendes til daglig leder. Vi skal sørge for at registrerte får gjennomført rettighetene sine hos oss.

Alle som spør har rett på grunnleggende informasjon om behandlinger av

personopplysninger i en virksomhet etter personopplysningslovens § 18, 1. ledd. TanaArbeidsservice AS har gitt denne informasjonen i denne erklæringen, og vil henvise til den ved eventuelle forespørsler. De som er registrert i en av TanaArbeidsservice AS sine systemer har rett på innsyn i egne opplysninger. Vedkommende har også rett til å be om at uriktige, ufullstendige eller opplysninger TanaArbeidsservice AS ikke har adgang til å behandle blir rettet, slettet eller supplert. Krav fra den registrerte skal besvares kostnadsfritt og senest innen 30 dager. For å be om innsyn, sletting, endring eller supplering kan du sende en e-post til postmottak@tana-arbeidsservice.no

10. Sletting av personopplysninger

Vi 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 vi gjennomgå dette. Våre retningslinjer for sletting følger av kartleggingsskjemaet.

Ansatte

Vi 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.

Deltakere på arbeidsmarkedstiltak AFT og VTA

Se ovenfor om behandlingsgrunnlaget for disse kategoriene. I henhold til Databehandleravtalen med NAV kreves det ved opphør av avtalen at:
Alle personopplysninger mottatt på vegne av NAV skal leveres tilbake til NAV.
Alle personopplysninger som er lagret elektronisk skal slettes.
Tana Arbeidsservice AS skal dokumentere at sletting er gjennomført.

Kontaktpersoner hos oppdragsgiver, samarbeidspartnere, leverandører og kunder

Vi skal slette opplysningene når vi blir kjent med at kontaktpersonen har sluttet hos oppdragsgiver, leverandøren eller kunden, eller når de har utpekt en ny kontaktperson. Det samme gjelder når samarbeidspartner/leverandør- eller kundeforholdet er opphørt.

Vi 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.

Andre kontaktpersoner

Vi skal slette opplysningene når vi blir kjent med at personen ikke lenger er relevant for våre behov, herunder hvis personen slutter hos den bedriften, offentlige etaten osv.

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

11. Personvernombud

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

For de fleste kategorier av registrerte behandler vi stort sett alminnelige bedriftsopplysninger, personopplysninger som navn, adresse, arbeidsgiver, e-postadresse, telefonnummer o.l. Vi behandler enkelte sensitive opplysninger om ansatte og tiltaksdeltakere.

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

12. Alminnelig risikovurdering

Vi skal risikovurdere behandlingen av personopplysninger. Denne vurderingen skal gjøre at vi er i stand til å identifisere og definere hvilke sikkerhetstiltak vi skal gjennomføre.

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.

Kartleggingsskjemaet viser at vi:

- I stor grad behandler bare alminnelige kontaktopplysninger, som navn, adresse, arbeidsgiver, e-postadresse, telefonnummer o.l.
- Behandler opplysninger om ansatte som er vanlige for å administrere personalforhold, herunder etterlevelse av lovpålagte forpliktelser
- Behandler opplysninger om deltakere i tråd med databehandler-avtalen med NAV

- Behandler opplysninger om elever og lærerkandidater etter avtale med utdanningsetaten
- Har en del privatkunder
- Ikke behandler opplysninger om barn
- Behandler opplysninger som er en del av det å drive alminnelig næringsvirksomhet

Vi har aldri vært utsatt for datainnbrudd. Vi er heller ikke kjent med at utenforstående har vist interesse for de personopplysningene vi behandler. Vi mener derfor at det er lite sannsynlig at opplysningene er utsatt for regelbrudd.

Når det gjelder en del av opplysningene om ansatte, lærerkandidater/elever eller tiltaksdeltakere, er både sannsynlighet for og alvoret ved regelbrudd større. Vi har derfor egne rutiner for behandling av slike opplysninger, herunder begrensning av tilgang til dem. Når det gjelder tiltaksdeltakere ivaretas behandlingen av personipplysninger I tråd med Databehandleravtalen med NAV.

Vi 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

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

Risikoene våre er vurdert overordnet i punktet ovenfor.

På denne bakgrunn har vi gjennomført disse tiltakene:

- Det er dagglig leder som skal påse at sikkerheten
- 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 virksomhetenes nettverk er beskyttet mot uvedkommendes bruk, eksempelvis ved sikring av trådløst nettverk.

- Ekstra tiltak skal iverksettes for spesielt beskyttelsesverdige opplysninger som for eksempel sykemeldinger, opplysninger rundt tilrettelegging av arbeidsplassen, vurderinger av den ansatte, merknader og advarsler.

- Ansatte skal gis opplæring i bruk av virksomhetens IT-system.

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

Avvik I henhold til personopplysningsloven og våre rutiner skal rapporteres til daglig leder. Den som oppdager avviket skal sammen med daglig leder iverksette tiltak hvis det er nødvendig for å begrense eller hindre vesentlige ulemper eller følgeskader, og at avviket ikke skjer igjen.

Den Vi må finne ut om behandlingen av personopplysninger følger reglene i personopplysningsloven og rutinene i dette dokumentet. Er det ikke tilfellet, må vi finne ut hvordan vi kan øke etterlevelsen. Vi skal dokumentere skriftlig både hvilke avvik vi har funnet og hva vi har gjort for å rette dem opp.

Ved avvik skal det rapporteres til Altinn:
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvikshandtering/melde-avvik-til-datatilsynet/

Viser det seg at rutinene ikke er godt nok tilpasset vår bedrift, bør vi vurdere å endre rutinene, se punkt 18.

15. Kjøp av IT-tjenester – databehandleravtaler

Vanligvis vil vi opptre som behandlingsansvarlig når virksomheten kjøper IT-tjenester fra en tjenesteleverandør. Vi har da fortsatt ansvaret for at personvernlovgivningen blir etterlevd ved kjøp av IT-tjenester, for eksempel Wis Tiltak, Net Ped, Zirius, ekstern server via Prodata og hjemmeside via Medianord.

Ved innkjøp av eventuelle nye IT-tjenester skal vi blant annet vurdere om leverandøren tilfredsstiller de kravene til sikkerhet som personopplysningsloven krever (artikkel 32). Seriøse leverandører vil ofte kunne dokumentere at de oppfyller kravene. Vi må også 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 vi straks kontakte Datatilsynet for å finne ut hva vi bør gjøre.

"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 vi varsle Datatilsynet og av og til også den registrerte. Varsling til Datatilsynet skal skje med én gang, og senest 72 timer etter at vi 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.

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

Vi skal dokumentere eventuelle brudd på personopplysnings sikkerheten. Dette gjør vi ved å beskrive de faktiske forholdene rundt bruddet ("Hva har skjedd?"). I tillegg skal vi beskrive virkningene av bruddet 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

Vi skal utrede personvernkonsekvensene når den 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 vi ta hensyn til arten, omfanget, sammenhengen og formålet med behandlingen. Den skal også ta hensyn til om den 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 vi sette oss 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

Vi skal oppdatere og revidere dette dokumentet jevnlig. Bakgrunnen er blant annet at reglene i lov og forskrift kan bli endret, vår behandling av personopplysninger kan bli endret eller erfaringer kan tilsi at vi bør endre rutinene våre. Av de samme grunnene skal vi også jevnlig gjennomgå og oppdatere skjemaene med kartlegging av behandling av personopplysninger, med dertilhørende risikovurdering.

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 en gang årlig.

Evalueringen bør omfatte:

- Har vi siden forrige revisjon endret (nye, endrede eller avsluttede) behandlinger av personopplysninger som ikke er behandlet i dokumentet eller i skjemaene?
- Tilsier de seks grunnkravene (punkt 5) 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