Personvern i Skjervøy Arbeidssamvirke AS

OM PERSONVERNDOKUMENTET 2

ANSVAR FOR BEHANDLING AV PERSONOPPLYSNINGER HOS OSS 2

KUNNSKAP OVER REGLENE OM PERSONOPPLYSNINGER 2

KARTLEGGING AV BEHANDLING AV PERSONOPPLYSNINGER 2

GRUNNKRAV FOR BEHANDLING AV PERSONOPPLYSNINGER 2

GRUNNLAG FOR Å BEHANDLE PERSONOPPLYSNINGER 3

- Behandlingsgrunnlag 3

JOBBSØKERE/ KANDIDATER OG ANDRE DELTAKERE I VÅRE PRIMÆRE TJENESTER 4

ORDINÆRE-, FASTE- OG MIDLERTIDIGE ANSATTE 4

- Ordinære ansatte 4
- Midlertidige ansatte 5
- Faste ansatte (Varig tilrettelagt arbeid) 5

TIDLIGERE ANSATTE 5

REKRUTTERING 5

KONTAKTPERSONER HOS EKSISTERENDE OG POTENSIELLE- BEDRIFTSKUNDER OG PRIVATKUNDER 6

KONTAKTPERSONER HOS EKSISTERENDE OG POTENSIELLE LEVERANDØRER 6

- Andre kontaktpersoner 7

GRUNNLAG FOR BEHANDLING AV SENSITIVE PERSONOPPLYSNINGER 7

INFORMASJON TIL DE REGISTRERTE (PERSONVERNERKLÆRING) 8

REGISTRERTES RETTIGHETER 8

SLETTING AV PERSONOPPLYSNINGER 8

- Ordinære og midlertidige ansatte 8
- Tidligere ansatte og jobbsøkere 8
- Tiltaksdeltakere, faste ansatte (varig tilrettelagt arbeid) og andre deltakere i vår primærtjeneste 8
- Kontaktpersoner hos leverandører og kunder 8
- Privatkunder 9
- Andre kontaktpersoner 9

PERSONVERNOMBUD 9

ALMINNELIG RISIKOVURDERING 9

INFORMASJONSSIKKERHET 10

AVVIK, ANALYSE AV AVVIK OG TILTAK FOR Å RETTE OPP I DEM 11
KJØP AV IT-TJENESTER – DATABEHANDLERAVTALER 11
BRUDD PÅ PERSONOPPLYSNINGSSIKKERHETEN 11
VURDERING AV PERSONVERNKONSEKVENSER OG FORHÅNDSKONSULTERING MED DATATILSYNET 12
KONTROLL, OPPDATERING OG REVISJON AV DOKUMENTET 12

Om personverndokumentet

Dette dokumentet skal bidra til at vi til enhver tid etterlever lov om personopplysninger. Dokumentet skal også bidra til å påvise at vår behandling av personopplysninger er i samsvar med lovverket.

Ansvar for behandling av personopplysninger hos oss

Bedriften er ansvarlig for personopplysninger vi behandler, for eksempel om egne ansatte, deltakere på tiltak, kontaktpersoner hos kunder og leverandører, privatkunder og andre forretningsforbindelser. Bedriften har ansvaret for å overholde de pliktene som følger av reglene om personopplysninger.

Det daglige behandlingsansvaret for faste ansatte, deltakere på tiltak og deltakere på andre primærtjenester innen attføring har attføringsavdelingen, og den enkeltes avdelingsleder. Det daglige behandlingsansvaret for ordinære ansatte, kunder, leverandører, privatkunder og andre forretningsforbindelser har daglig leder i virksomheten.

Kunnskap over reglene om personopplysninger

Vi skal sørge for at alle 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.

Kartlegging av behandling av personopplysninger

Vi skal kartlegge all behandling av personopplysninger. Dette skal gjøre vi i protokoller over behandlingsaktiviteter (artikkel 30) der vi angir blant annet kategorier av registrerte, formål med behandlingen, hvordan vi behandler opplysningene og hvilke grunnlag den har for behandlingen. Protokollene skal bidra til at vi etterlever reglene om behandling av personopplysninger.

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 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 konfidensialitet»)

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 7 «Vilkår for samtykke».

Grunnlag for å behandle personopplysninger

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.

Jobbsøkere/ kandidater og andre deltakere i våre primære tjenester

Vi behandler opplysninger om personer som deltar i våre tjenester innen Arbeid og inkludering.

For alle de arbeidsrettede tiltakene er NAV behandlingsansvarlig og det rettslige grunnlaget for behandlingen er «Forskrift om arbeidsrettede tiltak». Det er NAV som har satt formålet med behandlingen. I andre tilfeller kan det være fylkeskommuner eller kommuner som er behandlingsansvarlig. Da må disse kunne vise til et rettslig grunnlag for behandlingen.

Personopplysningene vi behandler er knyttet til dette avtaleforholdet. Det er i stor grad snakk om opplysninger jobbsøkere/ kandidater/ deltaker/ andre deltakere i våre primærtjenester har gitt oss.

Det rettslige grunnlaget i «Forskrift om arbeidsrettede tiltak» krever at vi utleverer opplysninger til NAV.

I henhold til databehandler avtale med NAV blir personopplysninger anonymisert innen 12 uker etter avslutning. Anonymiserte opplysninger slettes etter 12 måneder. Vi praktiserer dette for alle deltakere innen våre primærtjenester. Ansatte i Skjervøy Arbeidssamvirke AS får bare tilgang til opplysninger om deg hvis det er nødvendig for å behandle saken din. Tilgangen til opplysningene er sikret med tilgangskontroller. Når de ansatte jobber i datasystemene, blir oppslagene logget og kan spores i ettertid.

Ordinære-, faste- og midlertidige ansatte

Vi behandler personopplysninger om våre ordinære- og faste ansatte for å administrere vårt personale, for å organisere virksomheten vår, samt å overholde lovkrav.

Behandlingen av personopplysninger er basert på vår berettigede interesse som følger av at vi er arbeidsgiver. Vi behandler opplysninger også fordi vi er rettslig forpliktet til det, for eksempel til å utlevere og lagre opplysninger etter bokføringsloven, skatteforvaltningsloven og a-opplysningsloven. Noen få opplysninger må vi behandle for å oppfylle forpliktelser vi har i avtalen med de ansatte.

Ansatte er nødt til å gi oss de opplysningene vi trenger for formålene nevnt ovenfor.

Ordinære ansatte

Opplysninger blir lagret hos oss i elektroniske og fysiske personalmapper. Opplysninger er tilgjengelig kun for den aktuelle ansatte og daglig leder. Om opplysninger om navn og kontaktdetaljer skal deles, skal samtykkeerklæring benyttes.

Midlertidige ansatte
Opplysninger blir lagret hos oss i elektroniske og fysiske personalmapper. Opplysninger er tilgjengelig kun for den aktuelle ansatte, attføringsavdelingen, daglig leder, og den aktuelle ansattes avdelingsleder. Om opplysninger om navn og kontaktdetaljer skal deles, skal samtykkeerklæring benyttes.

Vi oppbevarer opplysninger om våre ordinære- og midlertidige ansatte for å kunne dokumentere vår etterlevelse av plikter som arbeidsgiver se. Tidligere ansatte.

Faste ansatte (Varig tilrettelagt arbeid)
Opplysninger blir lagret hos oss i elektroniske og fysiske personalmapper. Opplysninger er tilgjengelig kun for den aktuelle ansatte, attføringsavdelingen, daglig leder, og den aktuelle ansattes avdelingsleder. Om personopplysninger skal deles, skal samtykkeerklæring benyttes. Ansatte i Skjervøy Arbeidssamvirke AS får bare tilgang til opplysninger om deg hvis det er nødvendig for å behandle saken din. Tilgangen til opplysningene er sikret med tilgangskontroller. Når de ansatte jobber i datasystemene, blir oppslagene logget og kan spores i ettertid. I henhold til databehandler avtale med NAV blir personopplysninger for faste ansatte anonymisert innen 12 uker etter avslutning.

Tidligere ansatte
Vi behandler personopplysninger om tidligere ansatte for å kunne dokumentere vår etterlevelse av plikter som arbeidsgiver hvis det skulle bli nødvendig. Opplysninger om tidligere ansatte vil også fremgå av avtaler, korrespondanse og annen dokumentasjon vi lagrer og bruker som del av virksomheten vår.

Behandlingen av personopplysninger er basert på vår berettigede interesse i å dokumentere vår saksbehandling i egenskap som arbeidsgiver. Vi behandler opplysninger også fordi vi er rettslig forpliktet til det, etter bokføringsloven, skatteforvaltningsloven og a-opplysningsloven.

Rekruttering
Vi behandler personopplysninger om jobbsøkere for å vurdere om de er egnet for den stillingen de har søkt på.

Vi ber de som vil søke jobb hos oss om å sende oss minst opplysninger om navn, utdanning, arbeidserfaring, referansepersoner etc. (CV). Jobbsøkere vil ofte gi ytterligere personopplysninger de regner som relevante for vurderingen av søknaden. I intervjuer kan vi stille spørsmål for å avgjøre om jobbsøkeren passer til stillingen. Behandlingen av personopplysninger er basert på vår berettigede interesse i forbindelse med ansettelser og dokumentasjon av ansettelsesprosesser. Hvis det blir aktuelt å ansette jobbsøkeren vil vi kunne be om ytterligere informasjon samt om dokumentasjon for opplysninger vi allerede har fått. Ved ansettelse må jobbsøker fremvise politiattest iht. Forskrift om politiattest i henhold til arbeidsmarkedsloven. Det er frivillig å gi oss opplysninger. De opplysningene du velger å gi oss, vil ha betydning for vår vurdering av din søknad.

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.

Kontaktpersoner hos eksisterende og potensielle- bedriftskunder og privatkunder

Vi behandler opplysninger om kontaktpersoner hos eksisterende og potensielle bedriftskunder for markedsføring, salg, administrasjon, dokumentasjon og oppfølgning. Behandlingen av personopplysninger om bedriftskunder er basert på interesseavveining. Vi har behov for å holde kontakt med våre bedriftskunder for å følge opp 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 er kunde hos oss. I tillegg til navn behandler vi alminnelige opplysninger, som telefonnummer, epostadresse og arbeidsgiver, som alle er knyttet først og fremst til kontaktpersonens arbeidsforhold. Omfanget av opplysningene er derfor begrenset. Behandlingen av opplysningene er knyttet til leverandørens næringsvirksomhet og ikke til kontaktpersonens privatliv. Når det er påkrevet med samtykke etter markedsføringsloven, vil kontaktpersonen dessuten ha gitt samtykke før vi sender eposter med markedsføring. Vår behandling av personopplysningene er klart påregnelig for kontaktpersonen.

Vi behandler opplysninger om privatkunder for å fylle vår kontrakt med deg. Behandlingen skjer direkte overfor privatpersonen, som er kunde hos oss. I tillegg til navn behandler vi alminnelige opplysninger, som telefonnummer og epostadresse. Omfanget av opplysningene er derfor begrenset. Behandlingen av opplysningene er knyttet til privatkunden som oppdragsgiver og ikke til personens privatliv. Når det er påkrevet med samtykke etter markedsføringsloven, vil privatkunden dessuten ha gitt samtykke før vi sender eposter med markedsføring. Vår behandling av personopplysningene er klart påregnelig for privatkunden.

Behandlingen av personopplysninger er basert på vår berettigede interesse som består i behovet for å selge våre varer og tjenester. Vi lagrer og utleverer opplysninger også der vi har en rettslig forpliktelse til det, for eksempel etter bokføringsloven og skatteforvaltningsloven.

Det er frivillig for kontaktpersoner om de vil gi oss kontaktopplysninger, men av og til er det en betingelse for å inngå avtale at vi mottar de opplysningene vi trenger.

Vi lagrer opplysninger om deg, kun så lenge det er nødvendig for å oppnå formålet de ble innhentet for, eller dersom vi er pålagt å lagre opplysningene, eks. transaksjoner og betalingsinformasjon lagres i 5 år i henhold til bokføringsloven. Opplysningene vil slettes eller anonymiseres når de ikke lengre er nødvendige for å oppnå formålet.

Kontaktpersoner hos eksisterende og potensielle leverandører

Vi behandler personopplysninger om kontaktpersoner hos eksisterende og potensielle leverandører for forberedelser, administrasjon, dokumentasjon og oppfølgning.

Behandlingen av personopplysninger er basert på vår berettigede interesse som består i behovet for å kjøpe varer og tjenester. Vi lagrer og utleverer opplysninger også der vi har en rettslig forpliktelse til det, for eksempel etter bokføringsloven og skatteforvaltningsloven. Behandlingen skjer overfor kontaktpersonens arbeidsgiver, som ønsker å være leverandør hos oss. I tillegg til navn behandler vi kontaktopplysninger, som telefonnummer, epostadresse 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.

Det er frivillig for kontaktpersoner om de vil gi oss kontaktopplysninger, men av og til er det en betingelse for å inngå avtale at vi mottar de opplysningene vi trenger.

Vi lagrer opplysninger om deg, kun så lenge det er nødvendig for å oppnå formålet de ble innhentet for, eller dersom vi er pålagt å lagre opplysningene, eks. transaksjoner og betalingsinformasjon lagres i 5 år i henhold til bokføringsloven. Opplysningene vil slettes eller anonymiseres når de ikke lengre er nødvendige for å oppnå formålet.

Andre kontaktpersoner

Behandling av personopplysninger er basert på interesseavveining og rettslige forpliktelser. 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.

Grunnlag for behandling av sensitive personopplysninger

Behandling av sensitive personopplysninger krever behandlingsgrunnlag i tillegg til de som er nevnt i artikkel 6. Vi behandler opplysninger om personer som deltar i våre tjenester innen Arbeid og inkludering, og må behandle sensitive opplysninger for å oppfylle en rettslig forpliktelse ovenfor NAV. Alle som omfattes får samtykkeerklæring, som underskrives frivillig.

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 faste ansatte, tiltaksdeltakere og deltakere i andre primætjenester hos oss vil opplysninger om helse være særlig aktuelle. Helse omfatter for eksempel sykdom og skader og fravær begrunnet i dette. Særlig aktuelt behandlingsgrunnlag vil være at behandling er nødvendig for å utføre en rettslig forpliktelse ovenfor NAV eller utføre plikter som 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.

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. Informasjon til ansatte og tiltaksdeltakere gir vi i personalhåndbok eller lignende.

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.

Registrertes rettigheter

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

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

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 nedenfor.

Ordinære og midlertidige ansatte

Vi beholder som hovedregel alle opplysninger i hele ansettelsestiden, opplysninger blir lagret hos oss i elektroniske og fysiske personalmapper. Vi beholder opplysninger så lenge vi er rettslig forpliktet til det, for eksempel til å utlevere og lagre opplysninger etter bokføringsloven, skatteforvaltningsloven og a-opplysningsloven.

Tidligere ansatte og jobbsøkere

Vi behandler personopplysninger om tidligere ansatte for å kunne dokumentere vår etterlevelse av plikter som arbeidsgiver hvis det skulle bli nødvendig. Vi kan beholde opplysninger fra jobbsøkere i seks måneder, i tilfelle jobbsøkere skulle mene at deres rettigheter ikke er oppfylt.

Tiltaksdeltakere, faste ansatte (varig tilrettelagt arbeid) og andre deltakere i vår primærtjeneste

I henhold til databehandler avtale med NAV blir personopplysninger anonymisert innen 12 uker etter avslutning. Anonymiserte opplysninger slettes etter 12 måneder. Vi praktiserer dette for alle deltakere innen våre primærtjenester. Alle har rett til innsyn, retting og sletting.

Kontaktpersoner hos leverandører og kunder

Vi skal slette opplysningene når vi 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.

Vi lagrer opplysninger, kun så lenge det er nødvendig for å oppnå formålet de ble innhentet for, eller dersom vi er pålagt å lagre opplysningene, eks. transaksjoner og

betalingsinformasjon lagres i 5 år i henhold til bokføringsloven. Opplysningene vil slettes eller anonymiseres når de ikke lengre er nødvendige for å oppnå formålet.

Privatkunder

Vi skal slette opplysningene når kundeforholdet er opphørt.

Vi lagrer opplysninger, kun så lenge det er nødvendig for å oppnå formålet de ble innhentet for, eller dersom vi er pålagt å lagre opplysningene, eks. transaksjoner og betalingsinformasjon lagres i 5 år i henhold til bokføringsloven. Opplysningene vil slettes eller anonymiseres når de ikke lengre er nødvendige for å oppnå formålet.

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, offentlig etaten osv.

Vi lagrer opplysninger, kun så lenge det er nødvendig for å oppnå formålet de ble innhentet for, eller dersom vi er pålagt å lagre opplysningene, eks. transaksjoner og betalingsinformasjon lagres i 5 år i henhold til bokføringsloven. Opplysningene vil slettes eller anonymiseres når de ikke lengre er nødvendige for å oppnå formålet.

Personvernombud

Vi har vurdert at personvernforordningen ikke krever at vår bedrift skal ha personvernombud, da vi ikke driver regelmessig og systematisk monitorering i stor skala av registrerte. Men vi i Skjervøy Arbeidssamvirke AS tar personvern svært alvorlig. For de fleste kategorier av registrerte behandler vi personopplysninger som navn, adresse, arbeidsgiver, epostadresse, telefonnummer, fødselsnummer, kontonummer o.l. Vi behandler også enkelte sensitive opplysninger om ansatte som helseopplysninger.

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:

- Behandler sensitive opplysninger for å utføre en rettslig forpliktelse ovenfor NAV
- i stor grad behandler vi kontaktopplysninger, som navn, adresse, arbeidsgiver, epostadresse, telefonnummer, fødselsnummer, kontonummer og helseopplysninger o.l.
- Har databehandleravtaler med alle instanser som leverer programvare som inneholder personopplysninger

- behandler opplysninger om ansatte som er vanlige for å administrere personalforhold, herunder etterlevelse av lovpålagte forpliktelser

- 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 liten sannsynlig at opplysningene er utsatt for regelbrudd.

Basert på arten og omfanget av de opplysningene vi behandler i forbindelse med opplysninger om tiltaksdeltakere, deltakere i vår primærtjeneste, faste- og ordinære ansatte er både sannsynlighet for og alvoret ved regelbrudd stor. Vi har derfor egne rutiner for behandling av slike opplysninger, herunder begrensning av tilgang til dem.

Vi skal kontinuerlig risikovurdere endringer som kan påvirke informasjonssikkerheten, for eksempel når vi kjøper nye IT-tjenester og ved årlig risikovurdering.

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

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 utpekt en person hos oss med særlig oppgave å påse sikkerheten: Kvalitetsleder.

- 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.

- Ordinære ansatte skal gis grundig opplæring i bruk av virksomhetens IT-system.

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

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. Vi skal risikovurdere om behandlingen av personopplysninger er i henhold til lovverket, og kontinuerlig behandle avvik. Den som oppdager avviket skal registrere dette i vårt avvikssystem, og sette i gang umiddelbare tiltak hvis det er nødvendig for å begrense eller hindre vesentlige ulemper eller følgeskader. Den som mottar meldingen skal først vurdere om det er nødvendig med umiddelbare tiltak. Deretter skal vedkommende sørge for at det blir gjennomført tiltak som skal gjøre at avvik ikke skjer igjen.

Viser det seg at rutinene ikke er godt nok tilpasset vår bedrift, må vi vurdere å endre rutinene.

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.

Før vi kjøper IT-tjenester skal vi derfor blant annet vurdere om leverandøren tilfredsstiller de kravene til sikkerhet som personopplysningsloven krever etter artikkel 32. Seriøse leverandører vil ofte kunne dokumentere at de oppfyller kravene. Vi må også sørge for å inngå en databehandleravtale som regulerer hvordan leverandøren skal bla. håndtere kryptering, konfidensialitet, gjenoppretting av data og sikkerhetstiltak. 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.

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. 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.

I forbindelse med tiltaksdeltakere og faste ansatte (VTA) skal NAV også varsles, og det senest 24 timer etter at vi ble kjent med bruddet.

Vi har plikt til å varsle den registrerte dersom det er høy sannsynlighet for at bruddet på personopplysningssikkerheten vil medføre *høy* risiko for enkeltpersonenes rettigheter og friheter.

Vi skal dokumentere eventuelle brudd på personopplysningssikkerheten. 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.

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.

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 protokollene over behandlingsaktiviteter.

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

Evalueringen bør omfatte for eksempel på følgende spørsmål:

- Har vi siden forrige revisjon endret (nye, endrede eller avsluttede) behandlinger av personopplysninger som ikke er behandlet i dokumentet eller i protokollene?
- 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 protokollene?

- Har det kommet ny teknologi som gjør at personopplysninger kan sikres på en bedre måte