

Personvernerklæring Specto as

01.07.2022

1. Personvernsdokumentet

Dette dokumentet skal bidra til at bedriften etterlever lov om personopplysninger. Dokumentet skal også bidra til å påvise at vår behandling av personopplysninger er i samsvar med gjeldende lover og regler.

2. Ansvar for behandling av personopplysninger hos oss.

Specto er ansvarlig for personopplysninger som lagres og behandles hos oss. Eksempel på dette er egne ansatte, kontaktpersoner hos kunder og leverandører, privat kunder og andre forretningsforbindelser. Bedriften er godt kjent med lover og regler for GDPR. Bedriften har ansvaret for å overholde de plikter som følger av regler og lover om personopplysninger og sensitive opplysninger.

3. Kunnskap over reglene om personopplysninger.

Vi skal sørge for at ansatte har god kjennskap til reglene om personopplysninger, herunder dette dokumentet om personvern. Kunnskapsnivå skal være tilpasset den enkelte ansattes behandling av personopplysninger.

4. Kartlegging av behandling av personopplysninger.

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

5. Grunnleggende personvernprinsipper:

Reglene for *behandling av personopplysninger* bygger på noen grunnleggende prinsipper. Alle som behandler personopplysninger må opptre i samsvar med disse prinsippene.

A) Lovlig, rettferdig og gjennomiktig:

Behandling av personopplysninger må være lovlig.

Det må finnes et rettslig grunnlag for den behandlingen en virksomhet ønsker å gjøre. Forordningens artikkel 6 regulerer i hvilke tilfeller det skal anses lovlig å behandle personopplysninger. Minst ett av vilkårene i denne bestemmelsen må være oppfylt for at behandlingen er tillatt. Dersom det behandles *sensitive personopplysninger* må i tillegg minst ett av vilkårene i artikkel 9 være oppfylt.

B) Formålsbegrensning:

Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål.

Ethvert formål med *behandling av personopplysninger* skal identifiseres og beskrives presist. Alle formål skal være forklart på en måte som gjør at alle berørte har samme entydige forståelse av hva personopplysningene skal brukes til. At formålet skal være legitimt innebærer at det i tillegg til å ha et rettslig grunnlag også skal være i samsvar med øvrige etiske og rettslige samfunnsnormer.

C) Dataminimering:

Prinsippet om dataminimering innebærer å begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere innsamlingsformålet.

D) Riktighet

Personopplysninger som behandles skal være korrekte. Opplysningene skal også oppdateres hvis det er nødvendig.

E) Lagringsbegrensning

Prinsippet om lagringsbegrensning innebærer at personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for.

F) Integritet og konfidensialitet

Personopplysninger skal behandles slik at opplysningenes integritet og konfidensialitet beskyttes.

G) Ansvarlighet

Prinsippet om ansvarlighet understreker den behandlingsansvarliges ansvar for å opptre i samsvar med reglene for *behandling av personopplysninger*.

Det er ikke nok å bare ha ansvaret – man må vise at man tar ansvaret.

Den behandlingsansvarlige må opptre proaktivt og etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleves til enhver tid. Virksomheten må også kunne vise at den faktisk opptre i samsvar med reglene.

6. Grunnlaget for å behandle personopplysninger.

6.1 Behandlingsgrunnlag:

Specto skal ha minst ett av følgende grunnlag for all behandling av personopplysninger i bedriften:

- a)** Den registrerte har gitt samtykke til behandling av sine personopplysninger for ett eller flere spesifikke formål.
- b)** Behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på anmodning fra den registrerte før en avtaleinngåelse.
- c)** Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.
- d)** 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 grunnlag vi har for å behandle opplysninger.

Når grunnlaget for behandling er samtykke fra den registrerte (se p.k.t 6.1 a), 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 p.k.t 6.1 d), skal vi konkret og skriftlig dokumentere avveiningen.

6.2 Behandling av personopplysninger i forbindelse med gjennomføring av arbeidsmarkedstiltak.

I forbindelse med gjennomføring av arbeidsmarkedstiltak, ligger det rettslige grunnlaget i lov om arbeidsmarkedstjenester (arbeidsmarkedsloven), lov om arbeids- og velferdsforvaltningen (NAV loven) og forskrift om arbeidsmarkedstiltak, tiltaksforskriften.

Bedriftens rettslige grunnlag for å behandle personopplysninger i forbindelse med arbeidsmarkedstiltak er avledet av NAV's ansvar for å gjennomføre/organisere arbeidsmarkedstiltak.

NAV er behandlingsansvarlig og bedriften er databehandler.

Det rettslige forholdet mellom NAV og bedriften reguleres av databehandleravtalen.

Unntaket er tiltak der deltakere har et ansettelsesforhold (VTA).

Lønnsopplysninger, arbeidsavtaler, fraværsregistrering og eventuelt advarsler er personopplysninger som er knyttet til arbeidsforholdet og ikke selve tiltaksdeltakelsen.

For disse opplysningene er bedriften behandlingsansvarlig, mens det for opplysninger knyttet til tiltaksdeltakelsen er NAV behandlingsansvarlig og bedriften databehandler.

6.3 Ansatte:

Behandling av opplysninger er i hovedsak rettslige forpliktelser. Noe av behandlingen er også basert på interesseavveining. Vi har behov for å dokumentere at vi har oppfylt forpliktelser etter lov og avtale etter at de er oppfylt. Dette er berettigede interesser. Det er ikke mulig å ha tilgang til opplysningene på annen måte enn å lagre dem, behandling er derfor nødvendig. Ansatte hos oss har et løpende avtaleforhold med oss. Personopplysningene vi behandler er tilknyttet dette avtaleforholdet. Det er i stor grad snakk om opplysninger ansatte selv har gitt oss. Opplysningene gjelder forhold det er nærliggende at en arbeidsgiver behandler.

6.4 Tidligere ansatte:

Behandlingen av de fleste personopplysningene er basert på interesseavveining. Det kan oppstå behov for oss 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 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 12 måneder. Opplysninger om at den ansatte har vært ansatt, varighet av arbeidsforholdet og arbeidsoppgaver kan vi lagre lengre. Opplysningene vil ikke bli utlevert til andre uten at den tidligere ansatte ber om det, for eksempel i forbindelse med vurdering av ansettelse hos en ny arbeidsgiver.

6.5 Jobbsøkere:

Behandlingen av personopplysninger er basert på interesseavveining.

Vi har behov for å bruke opplysninger for å vurdere jobbsøknader. Dette er en berettiget interesse.

Det er ikke mulig å vurdere søknader uten å behandle personopplysninger. Behandling er derfor nødvendig.

Vi ber de som vil søke jobb hos oss om å sende oss opplysninger om navn, utdanning, arbeidserfaring, referansepersoner og CV.

Jobbsøkere vil ofte gi ytterligere personopplysninger de selv regner som relevante for vurderingen av deres søknad, for eksempel kontakt informasjon, familie forhold og interesser.

I intervjuer stiller vi spørsmål for å avgjøre om jobbsøkeren passer til stillingen. I noen tilfeller kan vi bruke 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. Vi bruker ikke opplysningene til noe annet enn å vurdere søknaden.

Vi gir ikke opplysningene til andre og kan beholde opplysninger fra jobbsøkere i 6 måneder, i tilfelle jobbsøkere skulle mene at deres rettigheter ikke er oppfylt.

6.6 Kontaktpersoner hos leverandører/bedriftskunder:

Behandlingen av personopplysninger er basert på interesseavveining. Vi har behov for å holde kontakt med våre leverandører for å følge opp blant annet bestillinger og leveranser. Dette er en berettiget interesse.

Den kontakten blir bare effektiv 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-post adresse, dette er knyttet først og fremst til kontaktpersonens arbeidsforhold og ikke til kontaktpersonens privatliv. Omfanget av opplysningene er svært begrenset.

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 kun være effektiv hvis vi kan kontakte enkeltpersoner direkte. Behandling er derfor nødvendig.

Vi lagrer navn og kontaktdetaljer og bruker opplysningene til å 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:

- helse
- opplysninger om rasemessig eller etnisk opprinnelse
- politisk oppfatning
- religion
- overbevisning
- fagforeningsmedlemskap
- genetiske opplysninger
- biometriske opplysninger
- seksuelle forhold eller seksuell orientering

Skal vi behandle slike opplysninger, skal vi sørge for å ha behandlingsgrunnlag. For ansatte hos oss vil opplysninger om helse være særlig aktuell. Helse omfatter for eksempel sykdom, skader og fravær begrunnet i dette.

Særlig aktuelt behandlingsgrunnlag vil være at behandling er nødvendig i egenskap av arbeidsgiver, for eksempel ved oppfølging og rapportering til offentlige myndigheter eller ved tilrettelegging av arbeidsforholdet. Behandling av opplysninger om straffbare forhold og lovovertridelser 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. Informasjon om personvern gir vi til ansatte, deltakere ved inntak og ansettelse.

Informasjonen skal inneholde blant annet:

- Navnet på bedriften
- Kontakt informasjon
- Formålet med behandlingen
- Kategoriene av personopplysninger
- Mottakere av personopplysninger (dersom de utleveres)
- Info om e.v.t utlevering av personopplysninger til andre land
- Hvor lenge personopplysningene lagres
- De registrertes rett til å kreve innsyn, rette eller slette personopplysningene
- Hvordan virksomheten fikk tilgang til personopplysningene
- Muligheten til å klage virksomheten inn til Datatilsynet.

9. Registrertes rettigheter:

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

10. Sletting av personopplysninger:

Vi skal slette personopplysninger uten ugrunnet opphold når de ikke lengre er nødvendig for formålet de ble samlet inn eller behandlet for. Vi skal gå igjennom dette minst `en gang i året for å kontrollere at personopplysningene er slettet.

Personer i tiltakene VTA og AFT Personopplysningene slettes etter 12 uker som er krav fra NAV.

Ansatte:

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

Tidligere ansatte og jobbsøkere:

Se ovenfor om behandlingsgrunnet for disse kategoriene. Lovgivning kan stille krav til lengre oppbevaring enn det som fremgår der.

Kontaktpersoner hos leverandører og kunder:

Vi skal slette opplysningene når vi er kjent med at kontaktpersonen har sluttet hos leverandøren eller at kunde/leverandør har utpekt ny kontaktperson. Det samme gjelder når leverandør- eller kundeforhold er opphørt. Andre kontaktpersoner Vi skal slette opplysningene når vi er kjent med at personen ikke lengre er relevant for våre behov, herunder hvis personen slutter hos bedriften, den offentlige etaten osv.

11. Personvernombud. Vi har en løpende vurdering på om vår bedrift skal ha et eget personvernombud. Vi tar behandlingen av sensitive personopplysninger svært alvorlig, og den enkelte ansatte er informert om våre prosedyrer og er ansvarlig for håndteringen av dette.

12. Alminnelig risikovurdering.

Vi skal gjennomføre en risikovurdering av behandlingen av personopplysninger.

Denne vurderingen skal gjøre oss 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, 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 vår primærtjeneste behandler sensitive opplysninger.
- Behandler opplysninger om ansatte som er vanlige for å administrere personalforhold, herunder etterlevelse av lovpålagte forpliktelser.
- Behandler opplysninger som en del av det å drive alminnelig næringsvirksomhet.
- Påser at datasikkerheten blir ivaretatt i alle ledd. Personvernerklæring Dato:

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.

Risikoene våre er vurdert overordnet i punkt 12.

På bakgrunn av dette har vi gjennomført disse tiltakene:

- Datasystem som gir mulighet for å spore endringer, hvem som har endret, til hvilket tidspunkt og i tillegg vise hvem som har lest i dokumentet og når dette skjedde
- Begrenset tilgang der arbeidsleder eller veileder har kun tilgang til de personopplysninger som er relevant for gjennomføringen av tiltaket
- Dataleverandør som har backup-system, som sikrer at opplysninger lagret i filer/dokument ikke går tapt.
- All lagring i eksterne servere er sikret med personlige tilgangskontoer som har to trinns innloggingsprosess.
- Ansatte skal gis opplæring i bruk av virksomhetens IT-system.
- Uvedkommende skal ikke ha tilgang til personopplysningene eller utstyr disse er lagret på.

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

Bedriften har eget avvikssystem som også omfatter IT-sikkerhet og personvern.

15. Kjøp av IT- tjenester – Databehandleravtaler:

Vi vil opptre som databehandleransvarlig når virksomheten kjøper IT- tjenester fra en tjenesteleverandør. Vi har da fortsatt ansvaret for at personvernlovgivningen blir etterlevd.

Før vi kjøper IT- tjenester skal vi vurdere om leverandøren tilfredsstillter kravene til sikkerhet som personopplysningsloven krever. Leverandør skal kunne dokumentere at de oppfyller kravene.

Dersom tjeneste leverandøren 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 ved et hackerangrep, skal vi melde dette inn til Datatilsynet og politiet.

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

Vi skal dokumentere eventuelle brudd på personopplysningssikkerheten. Dette gjør vi ved å beskrive de faktiske forholdet rundt hendelsen. I tillegg skal vi beskrive virkningene dette førte til og hvilke tiltak som er tatt for å avhjelpe bruddet. Denne dokumentasjonen gjør det mulig for Datatilsynet å kontrollere at virksomheten har etterlevd kravene i loven.

17. Kontroll, oppdatering og revidering 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.

Daglig leder har ansvaret for at endringer og revisjoner blir identifisert og innarbeidet i dette dokumentet. Dette gjøres årlig.

Besøk oss på internett. www.specto.no

Våre verdier: Respekt - Inkluderende - Mot - Tydelighet - Humor - Lønnsomhet.