GDPR-policy Metrostav Norge AS

1. Innledning

Metrostav Norge AS er forpliktet til å beskytte retten til personvern for sine ansatte og alle leverandørene vi samarbeider med. Formålet med dette dokumentet er å fastsette prinsippene for hvordan personopplysninger skal håndteres i samsvar med gjeldende personvernlovgivning. Dette inkluderer EUs personvernforordning 2016/679 ("GDPR").

Personvernrådgiveren i Metrostav Norge AS er ansvarlig for å iverksette og overvåke prosedyren.

2. Retningslinjer for databeskyttelse

2.1. Generelt

Vi behandler personopplysninger i samsvar med følgende prinsipper som er fastsatt i gjeldende personvernlovgivning.

2.2. Hovedprinsipper

Prinsipp 1: Lovlighet, rettferdighet og åpen informasjon

Rettferdig behandling: Vi skal avstå fra å behandle personopplysninger på en måte som er urimelig skadelig, uventet eller villedende for de berørte personene.

Åpen håndtering: Vi skal være tydelige, åpne og ærlige overfor de registrerte når det gjelder behandling og lagring av data, vi skal informere om hvilke formål og hvordan vi behandler personopplysningene. Lovlighet: Vi vil sørge for at all behandling av personopplysninger har et rettslig og lovlig grunnlag.

Prinsipp 2: Formålsbegrensning

Vi behandler bare personopplysninger for spesifikke, uttrykkelige og legitime formål.

Spesifikke og eksplisitte: Vi vil spesifisere formålet med hver behandlingsaktivitet.

Legitimt: Formålet må være berettiget i forhold til vår virksomhet.

Vi vil ikke behandle personopplysninger for formål som er uforenlige med det opprinnelige formålet som personopplysningene ble samlet inn for.

Vi kan behandle anonyme opplysninger uten begrensninger fordi de ikke lenger er personopplysninger.

Prinsipp 3: Dataminimering

Vi vil kun behandle de som er relevante og nødvendige, og vi vil gjøre det sånn:

• Identifisere hvilke typer personopplysninger som behandles, slik at vi kan vurdere nødvendigheten av opplysningene.

• Vi instruerer de ansatte om å unngå bruk av identifikatorer (der det er praktisk mulig) og å begrense mengden personopplysninger i dokumenter og skjemaer, enten de er elektroniske eller trykte.

Prinsipp 4: Datanøyaktighet

Vi vil iverksette egnede tiltak for å sikre at personopplysningene er nøyaktige, fullstendige og, der det nødvendig, oppdaterte. For å oppnå dette:

• vi vil innføre egnede prosedyrer for innsamling av personopplysninger for å sikre at opplysningene er korrekte.

• Vi vil innføre hensiktsmessige prosedyrer for regelmessig eller ad hoc-kontroll av systemer og dokumenter som inneholder personopplysninger som krever vedlikehold, for å sikre at opplysningene er oppdaterte.

• vi vil innføre hensiktsmessige prosedyrer for å gjøre det mulig for de registrerte å be om innsyn i personopplysningene og å be om retting, komplettering og oppdatering av personopplysningene.

Prinsipp 5: Begrensning av lagring

Vi vil ikke oppbevare personopplysninger lenger enn det som er nødvendig for det formålet de ble samlet inn for. For å gjøre dette:

• vil vi spesifisere den forventede lagringsperioden (dvs. når personopplysningene må slettes), inkludert årsaken til lagringsperioden.

• vi iverksetter automatiske sletteprosedyrer i rimelig omfang.

• Hvis sletterutinene skal være manuelle, må det iverksettes tidsplanlegging, varslingssystemer eller andre mekanismer for å sikre at rutinene overholdes.

• Vi støtter bruk av arkiverings- og kommunikasjonssystemer/plattformer for å redusere ustrukturerte data.

• der personopplysningene oppbevares for latente formål (f.eks. for å forsvare mulige krav), men som ellers ikke er nødvendige for den daglige driften, vil det bli truffet egnede tiltak for å begrense tilgangen til opplysningene og hindre at de brukes i den daglige driften (sperring eller begrensning av tilgangen). Der det er, vil disse arkiverte dataene bli pseudonymert (avidentifisert, f.eks. ved å erstatte navn/ID-identifikator).

• vil vi vurdere anonymisering som et alternativ til sletting dersom opplysningene fortsatt kan tjene et formål i anonymisert form. Anonymisering betyr at det er usannsynlig at opplysningene kan identifiseres på nytt på vanlig måte.

• hvis systembegrensninger krever at sikkerhetskopidata beholdes etter at oppbevaringsperioden er utløpt, må det sørges for at sikkerhetskopidataene er underlagt streng tilgangskontroll og ikke brukt i driften.

Prinsipp 6: Integritet og konfidensialitet

Vi vil sørge for tilstrekkelig sikkerhet for som beskrevet nedenfor.

3. Juridisk grunnlag

3.1. Generelt

Vi identifiserer det gjeldende rettslige grunnlaget for hver behandlingsaktivitet. Hvis det ikke kan identifiseres noe gyldig rettslig grunnlag, avsluttes aktiviteten.

For behandling av personopplysninger som ikke er særlige kategorier av personopplysninger (sensitive), kan vi påberope oss ett av følgende rettslige grunnlag i henhold til artikkel 6 i personvernforordningen:

Juridisk grunnlag	Beskrivelse	Krav	Eksempler på bruk
Avtale	Behandlingen av opplysningene er nødvendig for å oppfylle en avtale med den registrerte eller for ta skritt før inngåelse av en slik kontrakt.	Avtalen må inngås med de registrerte. På dette rettslige grunnlaget kam det ikke stoles på når det gjelder en avtale med kommersielle partnere (juridiske personer).	Rekruttering HR-administrasjon Lønn
Legitime interesser	Behandlingen av opplysningene er nødvendig for å oppnå en berettiget interesse, i den grad den går ut over dette interesser ikke går foran de registrertes rettigheter og interesser.	En legitim interesse er identifisert av oss eller en (f.eks. en kommersiell partner); opplysningene er nødvendige for å oppnå interessen; og, etter å ha tatt hensyn til interessene til den berettigede interessen er viktigere enn den registrertes rettigheter og interesser.	Kontrakts forvaltning med kommersielle aktører Partnere Fusjoner og oppkjøp HR-administrasjon Lønnsadministrasjo n
Juridiske forpliktelser	Behandlingen av opplysningene er nødvendig for å oppfylle en rettslig forpliktelse fastsatt i lovene i EU/EØS-landene.	Den rettslige forpliktelsen må være uttrykkelig eller implisitt fastsatt i lovgivningen i en EU/EØS-medlemsstat.	Regnskapssikkerhet
Vitale interesser	Databehandling er nødvendig for å beskytte vitale den registrertes interesser	Spørsmålet om liv og død	Beredskap
Offentlig interesse	Behandlingen av opplysningene er nødvendig for å utføre de oppgavene som utføres av en offentlig myndighet eller privat organisasjoner som handler allmennhetens interesse.	Utøvelse av offentlig myndighet.	Offentlig informasjon
Juridisk grunnlag	Beskrivelse	Krav	Eksempler på bruk

Samtykke	Den registrerte har samtykket til behandlingen.	Samtykke må gis i samsvar med GDPR artikkel 7.	Bruk av bilder av ansatte på intranett eller Internett Lagring av data på som ikke får etter rekrutteringsprosessen

3.2. Sensitive data

I tillegg må vi ha et rettslig grunnlag i henhold til artikkel 9 i personvernforordningen for spesielle kategorier av opplysninger (sensitive opplysninger). Sensitive opplysninger er opplysninger som avslører rasemessig eller etnisk opprinnelse, politisk oppfatning, religiøs eller filosofisk overbevisning eller fagforeningsmedlemskap, og behandling av genetiske opplysninger, biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Når vi behandler disse sensitive personopplysningene, identifiserer vi ett av følgende rettslige grunnlag:

Juridisk grunnlag	Beskrivelse	Krav	Eksempel på bruk
Sysselsetting	Behandlingen av opplysningene er nødvendig for å oppfylle forpliktelser og utøve spesifikke rettigheter innen arbeidsrett og lov om sosial trygghet og sosial beskyttelse.	Den må være godkjent i henhold til lov i hvert enkelt EU/EØS-land.	Håndtering av sykefravær. Tilpasning av arbeidsplassen av helsemessige årsaker. Alkohol- eller narkotikatester på arbeidsplassen, hvis det kreves av av sikkerhetsmessige årsaker.
Livsinteresser	Databehandling er nødvendig for å beskytte vitale den registrertes interesser i tilfelle den registrerte ikke er i stand til å gi samtykke.	Spørsmålet om liv og død	Beredskap

Offentlige data	Databehandlingen gjelder personopplysninger som den registrerte tilsynelatende oppgir	Den registrerte måtte helt klart utlevere opplysningene.	Public relations (f.eks. håndtering av en persons offentliggjorte partitilhørighet).
Juridisk grunnlag	Beskrivelse	Krav	Eksempel på bruk
Juridiske forpliktelser	Behandlingen er nødvendig for å fastsette, gjøre gjeldende eller forsvare rettskrav.	Kravet kan støttes på lov, avtale eller annet.	Svare på bindende innkallinger fra offentlige myndigheter.
Samtykke	Den registrerte er enig med ved å behandle personopplysningene.	Samtykke må gis i samsvar med GDPR artikkel 7.	Tilgangskontroll fra entreprenører.

3.3. Straffeforfølgelse og domfellelse

Vi kan bare behandle personopplysninger knyttet til straffbare handlinger og domfellelser hvis de har et rettslig grunnlag, enten samtykke, vital interesse eller rettslige krav som beskrevet ovenfor.

Opplysninger om straffedommer er opplysninger om personer som er idømt, bøter eller andre strafferettslige sanksjoner av domstolene (eller tilsvarende kompetente myndigheter), samt spørsmål og svar om hvorvidt en person har et rulleblad eller ikke. Strafferettslige opplysninger er opplysninger knyttet til siktelser eller straffesaker.

3.4. Unike identifikatorer

Vi kan bare behandle fødselsnummer og andre unike identifikatorer når det er et legitimt behov for spesifikk identifikasjon og metoden er nødvendig for å oppnå slik identifikasjon. Vi behandler ikke personnummer og andre unike identifikatorer for verifiseringsformål.

4. Åpenhet

4.1. Generelt

Vi skal være åpne om alle databehandlingsaktiviteter og gi de registrerte all informasjon om databeskyttelse.

4.2. Innholdet i personvernsinformasjonen

Vi vil informere de registrerte om hvorfor og hvordan opplysningene deres behandles, i samsvar med artikkel 13 og 14 i personvernforordningen. Informasjonen må være klar og utvetydig. Personvernsinformasjonen vil bli gjennomgått regelmessig for å sikre at den er oppdatert.

4.3. Formidling av informasjon om databeskyttelse

Vi vil sørge for at informasjon om personvern er lett tilgjengelig, for eksempel i kontrakter og på nettstedet vårt. Vi vil også gi relevant informasjon om personvern på forespørsel fra den registrerte.

4.4. Den registrertes rettigheter

Vi vil respektere de registrertes rettigheter i forbindelse med databehandling, herunder retten til innsyn, retting, sletting, begrensning og retten til å protestere.

4.5. Automatisert beslutningstaking

Vi kan bruke automatiserte avgjørelser, inkludert profilering, som har rettsvirkninger for eller på lignende måte påvirker de registrerte. Et eksempel er automatisert vurdering av jobbsøknader i

rekrutteringssammenheng. Vi vil overholde kravene i artikkel 22 i personvernforordningen for slike avgjørelser.

4.6. Markedsføring

Vi kan gjennomføre begrensede markedsføringsaktiviteter. Vi kan sende direkte markedsføring via e-post til følgende mottakere: de som har samtykket, eller de som er eksisterende forretningspartnere. Mottakerne vil ha mulighet til å reservere seg mot fremtidig e-postmarkedsføring.

4.7. Innebygd personvern og personvern som standardinnstilling

Når vi utvikler (internt eller gjennom tjenesteleverandører) programvare, plattformer eller andre løsninger, vil vi iverksette egnede tiltak for å iverksette retningslinjer for databeskyttelse som en integrert funksjon. Vi vil konfigurere slike løsninger slik at de som standard begrenser mengden personopplysninger, omfanget av databehandlingen og oppbevaringsperioden til et minimum.

4.8. Felles kontroll

Felles kontroll foreligger når to eller flere behandlingsansvarlige i fellesskap bestemmer formålene med og midlene for behandlingen, enten innenfor konsernet eller med hensyn til eksterne forretningspartnere.

Når vi (som behandlingsansvarlige) samarbeider med en eller flere andre behandlingsansvarlige (eller ekstern enhet) i forbindelse med behandling av personopplysninger, vil det bli vurdert fra sak til sak om de opptrer som felles behandlingsansvarlige. Som et utgangspunkt for en slik vurdering vil vi anse felles kontroll som sannsynlig hvis partene forfølger de samme overordnede målene og bidrar gjensidig til behandlingen av data.

Hvis det foreligger felles kontroll, vil det bli inngått en avtale felles administrator. En slik avtale vil identifisere partenes respektive ansvar for overholdelse av gjeldende lover og forskrifter, inkludert plikten til å gi informasjon om personvern til de registrerte, rollene og ansvaret overfor de registrerte med hensyn til håndtering av forespørsler om de registrertes rettigheter.

5. Overføring til land utenfor EU/EØS

Alle land i EU/EØS-området har iverksatt personvernforordningen for å sikre korrekt håndtering av personopplysninger.

For å kunne overføre eller behandle personopplysninger utenfor EU/EØS, må det sikres et passende beskyttelsesnivå. Dette kan sikres ved å overholde standardreglene som er vedtatt av EU- kommisjonen (standard kontrakts klausuler).

6. Databehandlere med personopplysninger

Vi bruker følgende firetrinns tilnærming for å engasjere prosessorer:

Trinn 1: Bestem rollene

Først avgjør vi om enheten opptrer som en databehandler. En databehandler er et selskap som behandler personopplysninger for oss uten selv å bestemme hvorfor behandlingen finner sted, hvilke opplysninger som skal behandles, og hvor lenge opplysningene skal oppbevares.

Trinn 2: Screening

Før vi engasjerer en databehandler, vil vi verifisere at databehandleren sørger for tilstrekkelige garantier for å oppfylle kravene i gjeldende personvernlovgivning. Vi kan gjøre dette ved å be om relevant dokumentasjon og informasjon om databeskyttelse i anskaffelsesprosessen eller på andre egnede måter.

Trinn 3: Inngåelse av databehandleravtalen

Vi vil inngå en med hver databehandler. Slike kontrakter kan komme i tillegg til en annen kontrakt (for eksempel en servicekontrakt).

Trinn 4: Revisjon

Vi vil kontrollere at databehandleravtalen overholdes.

Vi kan be databehandleren om å utarbeide regelmessige datasikkerhetsrapporter. Vi vil gjennomgå rapporten og vurdere om datasikkerhets- og personverntiltakene er tilstrekkelige. Hvis rapporten avdekker faresignaler, vil vi be om ytterligere informasjon. Hvis vi har grunn til å tro at databehandlerens datasikkerhets- eller personvernstandarder er utilstrekkelige, vil vi gjennomføre en grundigere revisjon. Hvis vi ikke er fornøyde med nivået på datasikkerheten eller personvernstandardene, avslutter vi kontrakten.

7. Deling av data med uavhengige administratorer

Når vi som behandlingsansvarlig deler personopplysninger med en annen separat behandlingsansvarlig, vil vi vurdere å formalisere dette avtale om beskyttelse av personopplysninger mot ulovlig behandling.

Når vi som behandlingsansvarlig mottar personopplysninger fra en annen uavhengig behandlingsansvarlig, vil vi vurdere å pålegge den behandlingsansvarlige en kontraktsmessig forpliktelse til å varsle de registrerte om at vi er mottaker av personopplysningene for å støtte den behandlingsansvarlige i samsvar med GDPR artikkel 13.

8. Registreringer av behandlingsaktiviteter

Vi vil etablere en liste over behandlingsaktiviteter. Formålet med disse fortegnelsene er å sikre etterlevelse av personvernforordningen artikkel 30 og gjøre det enklere å oppfylle andre krav i personvernforordningen. Arbeidstilsynets mal vil bli brukt til å opprette fortegnelser over behandlingsaktiviteter.

Det er den enkelte databehandlers ansvar å fylle ut og vedlikeholde slike registre. Databehandlingseieren er en rolle som har et funksjonelt ansvar.

9. Datasikkerhet

Vi vil iverksette og opprettholde egnede tekniske og organisatoriske tiltak for å sikre et tilstrekkelig datasikkerhetsnivå for å forhindre utilsiktet eller ulovlig ødeleggelse, tap, endring, uautorisert utlevering av eller tilgang til personopplysninger som overføres, lagres eller behandles på annen måte.

Når det gjelder personopplysninger, vil vi sørge for at datasikkerhetstiltakene tar behørig hensyn til følgende aspekter:

Sikkerhetskriterier	Definisjon av	Beskrivelse / Eksempler
Konfidensialitet	Beskyttelse mot uautorisert tilgang til eller utlevering av data.	1. Ansatte og forretningspartnere vil være underlagt en rimelig taushetsplikt. 2. Databasene vil være krypterte og underlagt passende tilgangskontroller. 3. Avtaler med IT-leverandører vil omfatte forpliktelser om datasikkerhet. 4. Fysiske fasiliteter skal være tilstrekkelig beskyttet mot uautorisert tilgang.
Integritet	Beskyttelse mot uautorisert endring eller sletting av data.	1. Databasene vil være krypterte og underlagt passende tilgangskontroller. 2. Sentrale dokumenter vil ha versjonskontroll (revisjonshistorikk).
Tilgjengelighet	Tilgang til data.	1. Avtaler med viktige leverandører av IT-tjenester skal ha hensiktsmessige vilkår og betingelser. 2. Materialdataene vil være eksternt tilgjengelige (VPN eller lignende).
Motstandsdyktighet	Kontinuitet i virksomheten sikres	1. Avtaler med viktige leverandører av IT-tjenester skal ha hensiktsmessige kommersielle vilkår. 2. Dataene vil bli sikkerhetskopiert.

10. Håndtering av datalekkasjer

Vi kan mulig oppleve brudd på personopplysningssikkerheten - et sikkerhetsbrudd som fører til utilsiktet eller ulovlig ødeleggelse, tap, endring, uautorisert utlevering av eller tilgang til personopplysninger. Hvis dette , vil vi innen 72 timer vurdere om vi må varsle de registrerte og/eller den relevante datatilsynsmyndigheten.

Ansatte som mistenker eller blir oppmerksomme på uønskede hendelser knyttet til behandling av personopplysninger, skal umiddelbart rapportere hendelsen til sin nærmeste leder, HR-leder eller personvernrådgiveren. Personvernrådgiveren er ansvarlig for å informere den kompetente datatilsynsmyndigheten.

11. Risikovurdering av personvern

Vi vil jevnlig gjennomføre generelle vurderinger av personvernrisikoen i virksomheten vår. Formålet med slike vurderinger er å identifisere mulige personvernrisikoer og å identifisere tiltak som er egnet til å minimere disse risikoene. I forbindelse med personvern er risikoene (negative konsekvenser av en hendelse) spesielt: Fysisk skade, diskriminering, identitetstyveri, bedrageri, økonomisk tap, skade på omdømme; økonomisk eller sosial ulempe; uautorisert avsløring av eller tilgang til spesielle uautorisert utlevering av eller tilgang til opplysninger om personlige forhold som økonomisk situasjon eller evaluering av arbeidsprestasjoner.

Risikovurderingen skal minst ta hensyn til: (i) nivået for akseptabel risiko, (ii) mulige uønskede hendelser, (iii) sannsynligheten for at disse hendelsene inntreffer, (iv) personvernkonsekvensene hvis hendelsen inntreffer, og (iv) hvis risikoen er uakseptabel, tiltak for å håndtere risikoen.

12. **Konsekvensanalyse av databeskyttelse**

Hvis en prosessering, for eksempel bruk av en ny teknologi, sannsynligvis vil resultere i en høy personvernrisiko, med tanke på dens art, omfang, kontekst og formål, vil vi gjennomføre en vurdering av personvernkonsekvenser (DPIA).

Personvernkonsekvensvurderingen må minst inneholde (i) en systematisk beskrivelse av planlagte behandlingen, (ii) en vurdering av nødvendigheten og forholdsmessigheten av behandlingen, (iii) en vurdering av personvernrisikoen og (iv) tiltak for å håndtere risikoen.

13. Identifisering av hoved tilsynsmyndighet

Når det kreves kommunikasjon med en tilsynsmyndighet i forbindelse med grenseoverskridende behandling som involverer mer enn ett EØS-land, må det utpekes en ledende tilsynsmyndighet.

Tilsynsmyndigheten er myndigheten i det landet der vår er lokalisert. Hovedvirksomheten skal være lokalisert der vi har vår sentraladministrasjon, med mindre beslutninger om formålene med og midlene for behandlingen tas ved en annen virksomhet som har myndighet til å ta slike beslutninger.

14. Opplæring

Vi vil gi våre ansatte opplæring i personvern og personvern.

Personell med permanent eller regelmessig tilgang til personopplysninger som er involvert i som samler inn personopplysninger eller utvikler verktøy som brukes til å behandle personopplysninger, får obligatorisk opplæring i personvern og databeskyttelse. Relevant personale bør defineres i henhold til deres eksponering for behandling av personopplysninger i forbindelse med deres stilling og daglige oppgaver. Relevant personell er:

• HR-avdeling som håndterer HR-data.

• Sikkerhetsfunksjoner, spesielt helse- og sikkerhetspersonell, personell som skal håndtere sikkerhetshendelser, inkludert identifiserte personer og beredskapsteam

• Konsernrevisjon

• IT-funksjoner, nærmere bestemt informasjonssikkerhet, applikasjonsstøtte og andre IT-tjenester

• Linjeledere