GE-HÅNDBOKA · RUTINE · 1.03 PERSONAL

Behandling av personopplysninger

Dokumentnr.	GE-1.03-30 R
Type	Rutine
Kapittel	1.03 Personal
Gjelder for	Alle ansatte i Gjerdalen Entreprenør AS som behandler personopplysninger
Revisjon / dato	Rev. 01 · Utkast
Utarbeidet av	HMS- og kvalitetsleder
Godkjent av	Daglig leder
Krav og grunnlag	Personopplysningsloven; GDPR art. 5, 6, 9, 13, 15–21, 28, 30, 32, 33 og 34; Arbeidsmiljøloven kap. 9; Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale
Erstatter	SmartDok 0103-042 R

1. Formål og omfang

Rutinen skal sikre at Gjerdalen Entreprenør AS, org.nr. 925 994 685, behandler personopplysninger lovlig og sikkert, i samsvar med det til enhver tid gjeldende regelverket: personopplysningsloven og personvernforordningen (GDPR).

Rutinen gjelder opplysninger om ansatte, søkere, innleide og ansatte hos underentreprenører, kontaktpersoner hos kunder og leverandører, og andre personer vi registrerer opplysninger om.

2. Ansvar

Rolle	Ansvar
Daglig leder	Har det juridiske ansvaret for at bedriften følger regelverket. Gjerdalen Entreprenør AS er behandlingsansvarlig, og daglig leder har ansvaret på vegne av bedriften. Sørger for at nye retningslinjer blir innført og fulgt.
HMS- og kvalitetsleder	Hjelper daglig leder med å holde kartleggingen av personopplysninger oppdatert, og følger opp avvik.
Prosjektleder	Sørger for at personopplysninger på prosjektene (mannskapslister, bilder, RUH, timer) behandles etter rutinen.
Alle ansatte	Setter seg inn i rutinen, påser at personopplysninger behandles etter den og etter regelverket, bruker bare opplysninger de trenger i jobben, og melder fra straks hvis opplysninger kommer på avveie.

3. Definisjoner

Begrep	Betydning
Personopplysning	En opplysning eller vurdering som kan knyttes til en enkeltperson. Eksempler er navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, fingeravtrykk og fødselsnummer (både fødselsdato og personnummer). Posisjonsdata og timeføring er også personopplysninger.
Ikke personopplysning	Opplysninger om en bedrift, som navn, organisasjonsnummer og bedriftens felles e-post og telefonnummer. Navn og kontaktinformasjon direkte til daglig leder eller andre kontaktpersoner er likevel personopplysninger.
Særlige kategorier (sensitive opplysninger)	Blant annet helseopplysninger, fagforeningsmedlemskap, etnisk opprinnelse og religion (GDPR art. 9). Opplysninger om straffbare forhold behandles med samme varsomhet.
Behandling	All bruk av personopplysninger: innsamling, registrering, lagring, deling og sletting.
Databehandler	En leverandør som lagrer eller bruker personopplysninger på vegne av Gjerdalen.

4. Arbeidsgang

4.1 Prinsipper

All behandling skal oppfylle prinsippene i GDPR art. 5:

1. Lovlig, rettferdig og åpen: den registrerte vet hva som behandles, og hvorfor.
2. Formålsbegrenset: formålet bestemmes før opplysningene samles inn.
3. Dataminimering: vi samler bare inn det vi trenger.
4. Riktighet: opplysningene holdes korrekte og oppdaterte.
5. Lagringsbegrensning: opplysningene slettes når de ikke lenger trengs.
6. Integritet og konfidensialitet: opplysningene sikres mot uvedkommende og mot tap.

4.2 Behandlingsgrunnlag

All behandling av personopplysninger i bedriften skal ha et lovlig behandlingsgrunnlag. GDPR art. 6 gir en uttømmende liste. Behandlingen er lovlig bare når minst ett av disse vilkårene er oppfylt:

- Den registrerte har gitt samtykke til behandling for ett eller flere bestemte formål.
- Behandlingen er nødvendig for å oppfylle en avtale den registrerte er part i (for eksempel arbeidsavtalen), eller for å gjennomføre tiltak den registrerte ber om før en avtale inngås.
- Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler Gjerdalen (for eksempel skattetrekk, a-melding, HMS-kort, mannskapslister og eksponeringsregister).
- Behandlingen er nødvendig for å verne den registrertes eller en annen persons vitale interesser.
- Behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet.
- Behandlingen er nødvendig for en berettiget interesse hos Gjerdalen eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran. Det gjelder særlig hvis den registrerte er et barn.

Gjerdalen skal fortløpende slette personopplysninger som bedriften ikke har behandlingsgrunnlag for.

4.3 Kartlegging

Gjerdalen skal kartlegge og ha oversikt over alle gruppene av personopplysninger som behandles (protokoll over behandlinger, GDPR art. 30). For hver gruppe skal kartleggingen vise

- behandlingsgrunnlag og formål,
- type personopplysning og opplysningenes omfang,
- ansvarlig i bedriften (system- eller dataeier),
- lagring og kommunikasjon,
- informasjonssikkerhet,
- databehandler.

Hvordan kartleggingen gjøres, står i **GE-1.03-32 D** Kartlegging av personopplysninger – forklaring. Hovedgruppene i Gjerdalen er:

Gruppe	System eller sted
Lønn og personaladministrasjon	Lønnssystem og Xledger
Personalmappe, arbeidsavtale, kompetanse	Personalmappen i SharePoint (begrenset tilgang) og SmartDok (kompetansematrise og CV-bank)
Timer, fravær, RUH, SJA, skjemaer og bilder	SmartDok
Mannskapslister og HMS-kort	SmartDok (mannskapsliste)
Posisjon og kjørebok for kjøretøy	ABAX, se **GE-1.02-31 R**
Sykefravær og tilrettelegging (helseopplysninger)	Personalmappen med begrenset tilgang, NAV
Eksponeringsregister og helseundersøkelser	Se **GE-1.03-33 R**
Varslingssaker	Se **GE-1.03-08 R**

4.4 Formål og informasjon

1. Før personopplysninger samles inn, skal behovet og formålet være definert.
2. Den enkelte skal på en enkel og lettfattelig måte få vite formålet med innsamlingen, og at personen har rett til innsyn og rett til å få opplysningene rettet eller slettet (GDPR art. 13).
3. Gjerdalen skal ha en personvernerklæring tilgjengelig for alle ansatte, se **GE-1.03-31 D** Personvernerklæring til ansatte.
4. Gjerdalen skal også ha en personvernerklæring på hjemmesiden, sammen med opplysninger om bruk av informasjonskapsler (cookies).
5. Opplysningene skal slettes fortløpende når formålet med behandlingen ikke lenger er aktuelt.

4.5 Sensitive personopplysninger (særlige kategorier)

Særlige kategorier, for eksempel helseopplysninger ved sykefravær, kan behandles når det er nødvendig for å oppfylle plikter etter arbeidsretten (GDPR art. 9 nr. 2 bokstav b). Ellers kreves samtykke fra den registrerte. I et arbeidsforhold er samtykke sjelden frivillig, og bør ikke være grunnlaget når en lovpålagt plikt er grunnlaget.

4.6 Kontrolltiltak overfor ansatte

- Posisjonssporing (for eksempel elektronisk kjørebok), kameraer og andre kontrolltiltak krever saklig grunn, skal ikke være uforholdsmessig belastende, og skal drøftes med de tillitsvalgte før de innføres (arbeidsmiljøloven kap. 9).
- Innsyn i e-post og filområder skjer bare etter forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale.

4.7 Rettighetene til de registrerte

Den registrerte har rett til innsyn, retting, sletting, begrensning og til å protestere (GDPR art. 15–21). Henvendelser rettes til daglig leder og besvares uten ugrunnet opphold, og senest innen én måned.

4.8 Korrigering og sletting

- Gjerdalen skal sørge for at personopplysningene som behandles, til enhver tid er korrekte. Feil rettes når de oppdages.
- Personopplysninger som behandles uten lovlig behandlingsgrunnlag, eller som ikke lenger har et klart definert formål, slettes, med mindre lov krever lengre oppbevaring (for eksempel bokføringsloven og eksponeringsregisteret).

4.9 Informasjonssikkerhet

Gjerdalen skal ha og følge gode nok rutiner for å hindre at personopplysninger kommer på avveie (GDPR art. 32). Det gjelder

- fysisk sikring, som adgangskontroll, låsing av kontor og alarmsystemer,
- datasikkerhet, som kryptering, passordbeskyttelse og personlige brukere,
- tilgang etter tjenstlig behov. Tilgang fjernes når noen slutter eller bytter rolle,
- at personalmapper og helseopplysninger bare lagres med begrenset tilgang, aldri i prosjektmapper eller på private enheter.

4.10 Databehandleravtaler

Gjerdalen skal bare bruke eksterne databehandlere som behandler personopplysninger i tråd med GDPR, og som kan dokumentere det skriftlig. Det skal inngås skriftlig databehandleravtale (GDPR art. 28) før databehandleren tas i bruk.

Databehandlere for Gjerdalen er blant annet leverandørene av SmartDok, Xledger, ABAX, ProAdm og Microsoft (SharePoint og Teams).

4.11 Brudd på personopplysningssikkerheten

1. Alle som oppdager at personopplysninger er kommet på avveie, er sendt feil eller kan være tilgjengelige for uvedkommende, melder straks fra til daglig leder.
2. Daglig leder vurderer risikoen og melder bruddet til Datatilsynet innen 72 timer, når det ikke er usannsynlig at bruddet gir risiko for de registrerte (GDPR art. 33).
3. Ved høy risiko varsles de som er berørt (GDPR art. 34).
4. Alle brudd registreres internt med årsak og tiltak, også de som ikke meldes til Datatilsynet.

5. Kontroll, registrering og dokumentasjon

Dokumentasjon	Ansvar
Kartlegging av personopplysninger (protokoll)	Daglig leder. Gjennomgås minst én gang i året.
Databehandleravtaler	Daglig leder
Logg over brudd på personopplysningssikkerheten	Daglig leder
Personvernerklæring til ansatte	Håndboka (**GE-1.03-31 D**)
Personvernerklæring og informasjonskapsler	Gjerdalens hjemmeside

6. Referanser

- Personopplysningsloven og personvernforordningen (GDPR)
- Arbeidsmiljøloven kap. 9 (kontrolltiltak)
- Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale
- Bokføringsloven
- **GE-1.02-31 R** Elektronisk kjørebok
- **GE-1.03-06 R** Personalopplysninger
- **GE-1.03-08 R** Varsling av kritikkverdige forhold
- **GE-1.03-29 D** Taushetserklæring
- **GE-1.03-31 D** Personvernerklæring til ansatte
- **GE-1.03-32 D** Kartlegging av personopplysninger – forklaring
- **GE-1.03-33 R** Register over eksponerte arbeidstakere

Revisjonshistorikk

Rev.	Dato	Endring	Godkjent av
01	Utkast	Første utgave i GE-håndboka. Skrevet om fra SmartDok 0103-042 R.	Daglig leder