GE-HÅNDBOKA · DOKUMENT · 1.03 PERSONAL

Kartlegging av personopplysninger – forklaring

Dokumentnr.	GE-1.03-32 D
Type	Dokument
Kapittel	1.03 Personal
Gjelder for	Daglig leder og andre i Gjerdalen Entreprenør AS som kartlegger og har ansvar for personopplysninger
Revisjon / dato	Rev. 01 · Utkast
Utarbeidet av	HMS- og kvalitetsleder
Godkjent av	Daglig leder
Krav og grunnlag	Personopplysningsloven; GDPR art. 6, 9, 28, 30 og 32
Erstatter	SmartDok 0103-044 D

1. Formål

Dokumentet forklarer hovedpunktene i kartleggingen av personopplysninger som Gjerdalen skal ha etter **GE-1.03-30 R** Behandling av personopplysninger. Hvert punkt under svarer til en kolonne i kartleggingen. Kartleggingen er Gjerdalens protokoll over behandlinger etter GDPR art. 30.

Daglig leder har ansvaret for at kartleggingen blir gjort og holdt oppdatert.

2. Gruppe personopplysning

Utgangspunktet for kartleggingen er de ulike gruppene av personopplysninger bedriften har. Det kan være arbeidsavtaler, de ansattes CV-er, kursbevis og sertifikater, e-poster fra kunder, opplysninger om kunder eller helseattester.

Er du i tvil om en opplysning er en personopplysning, se definisjonen i **GE-1.03-30 R**, eller les mer på Datatilsynets nettsider.

3. Formålet med å bruke eller lagre opplysningene

Ingen bedrift behandler personopplysninger for moro skyld. All bruk og oppbevaring av personopplysninger skal ha et aktverdig formål, og formålet bør dokumenteres. Klarer man ikke å svare på hva formålet med en gruppe personopplysninger er, bør opplysningene sannsynligvis slettes.

4. Opplysningenes omfang

Bedriften må definere hva personopplysningene skal og kan brukes til. Denne vurderingen henger sammen med formålet, og gjør det klart for bedriften hva opplysningene skal brukes til, og hva de ikke skal brukes til.

5. Behandlingsgrunnlag

Behandlingsgrunnlaget er hjemmelen for å behandle personopplysningene. Ta utgangspunkt i reglene i personopplysningsloven, slik de følger av GDPR art. 6. Behandlingen er bare lovlig 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, eller for å gjennomføre tiltak den registrerte ber om før en avtale inngås.
- Behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige.
- 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 som den behandlingsansvarlige har fått.
- Behandlingen er nødvendig for en berettiget interesse hos den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran. Det gjelder særlig hvis den registrerte er et barn.

6. Ansvarlig dataeier i bedriften

Alle personopplysninger skal ha en ansvarlig i bedriften (dataeier). Som regel er dette daglig leder. For arbeidsavtalene kan det for eksempel være den som har personalansvaret.

En tommelfingerregel er at dataeieren har rett til å kreve personopplysningene slettet. Dataeieren er som hovedregel daglig leder.

7. Type personopplysning

Bedriften må vurdere om personopplysningen er sensitiv (særlig kategori etter GDPR art. 9), for eksempel helseopplysninger. Sensitive opplysninger krever et særskilt grunnlag og ekstra sikring, se **GE-1.03-30 R**. Gir behandlingen høy risiko for de registrerte, skal det gjøres en vurdering av personvernkonsekvenser før behandlingen starter.

Bedriften må også beskrive i klartekst hva slags personopplysninger som er lagret. Gjelder det for eksempel e-poster på daglig leders e-postkonto (ustrukturerte data), kan det være navn, telefonnumre, e-postadresser, bostedsadresser, personnumre og lignende.

8. Lagring og kommunikasjon

Bedriften må beskrive hvor personopplysningene er lagret, for eksempel på en server, i en database eller et fagsystem, i et fysisk arkiv eller på en minnepinne.

9. Informasjonssikkerhet

Bedriften har ansvar for at personopplysningene ikke kommer på avveie. Bedriften må dokumentere at det er gode nok sikkerhetstiltak til å hindre at uvedkommende får tilgang til opplysningene.

1. Beskriv hvem i bedriften som har tilgang til opplysningene, og om de er lagret på en lokal datamaskin eller hos en ekstern leverandør av database eller server.
2. Beskriv hvilke sikringstiltak bedriften har for hver gruppe personopplysninger. Sentrale tiltak er opplæring av de ansatte i bruk og lagring av personopplysninger, kryptering og passordbeskyttelse av elektroniske dokumenter, og fysisk sikring med alarm, kameraovervåking og låste dører.

10. Databehandler

En databehandler lagrer eller bruker personopplysninger på vegne av den behandlingsansvarlige. Typiske databehandlere er leverandører av e-post og skylagring, servere, databaser og fagsystemer. For Gjerdalen gjelder det blant annet SmartDok, Xledger, ABAX, ProAdm og Microsoft (SharePoint og Teams), se **GE-1.03-30 R**.

Gjerdalen er selv ansvarlig for å inngå en databehandleravtale med hver databehandler (GDPR art. 28), der databehandleren forplikter seg til å behandle personopplysningene i tråd med GDPR. Mange leverandører har en standard databehandleravtale som en del av avtalevilkårene.

11. Avvik

Til slutt bør bedriften vurdere om kartleggingen har avdekket avvik fra kravene i personopplysningsloven. Et typisk avvik er at bedriften har personopplysninger som det egentlig ikke finnes et aktverdig formål med å lagre.

12. Tiltak

Avdekker kartleggingen avvik, må det gjøres tiltak for å lukke dem. Et mulig tiltak er å slette personopplysningene. Har bedriften for eksempel avdekket manglende adgangskontroll til kontorer der det lagres personopplysninger, kan tiltaket være en rutine for å låse kontorene når de ikke er i bruk.

13. Referanser

- Personopplysningsloven og personvernforordningen (GDPR)
- Datatilsynet: veiledning om personopplysninger og protokoll (datatilsynet.no)
- **GE-1.03-30 R** Behandling av personopplysninger
- **GE-1.03-31 D** Personvernerklæring til ansatte

Revisjonshistorikk

Rev.	Dato	Endring	Godkjent av
01	Utkast	Første utgave i GE-håndboka. Skrevet om fra SmartDok 0103-044 D.	Daglig leder