00.110 GDPR - Personvern

Hensikt

Personopplysningslovens bestemmelser gir de overordnede rammene for behandling av personopplysninger.

Prosedyren skal sikre at ansattes personopplysninger blir håndtert på en sikker og forsvarlig måte i forhold til gjeldende regelverk.

Da Personopplysningsloven og Personopplysningsforskriften stiller en rekke spesifikke krav til behandlingen og datasikkerheten, har Eid Elektro AS utarbeidet denne prosedyren for å beskrive hvordan disse kravene ivaretas.

Definisjon

Behandling av personopplysninger er regulert i lov om behandling av personopplysninger (personopplysningsloven) og tilhørende forskrift (personopplysningsforskriften).

Personopplysningsloven har til formål å beskytte enkeltpersoner mot at deres personvern blir krenket gjennom behandling av personopplysninger, jf. lovens § 1. Personopplysninger skal behandles i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet og privatlivets fred. Personvernbegrepet er ikke klart definert i loven, men er et samlebegrep som beskriver mange ulike interesser og verdier for enkeltindividet.

Omfang

Loven pålegger enhver virksomhet å sørge for at personopplysninger om egne ansatte og andre behandles på en forsvarlig måte. Etter personopplysningsloven § 14 er alle virksomheter pålagt å etablere og vedlikeholde planlagte og systematiske tiltak som er nødvendige for å oppfylle kravene i personopplysningsloven og personopplysningsforskriften, altså et internkontrollsystem.

Ansvar

Kjøllesdal Ove har det overordnede ansvaret for denne prosedyren. Som Eid Elektro AS øverste leder regnes vedkommende som behandlingsansvarlig for personopplysningene.

Den behandlingsansvarlige er etter personopplysningsloven § 2 nr. 4) og GDPR art. 4 nr. 7) den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Ved avgjørelsen av hvem som er å anse som behandlingsansvarlig i Eid Elektro AS, er det avgjørende hvem som har instruksjons- og delegasjonsmyndighet, herunder bestemmelsesrett over personopplysningene, den elektroniske behandlingen av disse og den aktuelle tilgangsstyringen i de elektroniske systemene.

Kjøllesdal Ove er ansvarlig for å utføre årlige ettersyn for å kontrollere at rutinene blir fulgt og at de er funksjonelle for de ansatte, om det har skjedd endringer i regelverket eller andre rammefaktorer, endringer i behandlingen av personopplysninger mv.

Beskrivelse

Eid Elektro AS sine behandlinger av personopplysninger skal ivareta følgende hensyn:

- Beskyttelse av den enkelte mot at personvernet blir krenket ved vår behandling av personopplysninger.

- Sikre at enkeltpersoner ved forespørsel får de opplysninger vedkommende har krav på etter personopplysningsloven.
- Sikre at personopplysningene som behandles er riktige, fullstendige og tilstrekkelig adekvate i forhold til formålet, at opplysningene lagres på en sikker måte, og ikke oppbevares lenger enn nødvendig.

De overordnede målene i Eid Elektro AS ivaretar samtlige av disse aspektene, med den presisering at ved behandling av sensitive personopplysninger skal sikring av konfidensialitet som hovedregel prioriteres foran prinsippene om integritet og tilgjengelighet.

Eid Elektro AS behandler kun personopplysninger om egne ansatte og våre private kunder.

For Eid Elektro AS egne ansatte behandles i hovedsak personopplysninger vi har en lovfestet plikt til eller som er nødvendige for å kunne utføre Eid Elektro AS arbeidsgiveransvar. Vi behandler i begrenset grad sensitive opplysninger i forbindelse med tariffestet plikt til forskuddstrekk av fagforeningskontingent og ved oppfølging av sykemeldte arbeidstakere.

Om private kunder oppbevares kun opplysninger som er nødvendige for at vi skal kunne gjennomføre avtalene med de respektive kundene, samt opplysninger vi er pålagt å oppbevare etter bokføringslovgivningen.

Omfanget av personopplysninger og kategorien av disse er av en slik karakter at de representerer en lav risiko for krenkelse av personvern.

I henhold til GDPR art. 30 skal den behandlingsansvarlige føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Protokollen skal inneholde:

- Formålene med behandlingen
- Beskrivelse av kategorier av registrerte og kategorier av

personopplysninger
- Kategorier av mottakere som personopplysninger er blitt eller vil bli utlevert til.
- Hvis mulig, forespeilte slettefrister for ulike kategorier av opplysninger
- Hvis mulig, generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak

Se vedlagt dokument “Protokoll_til_GDPR art 30”

Rutinene for rapportering av hendelser og håndtering av avvik skal sikre at Eid Elektro AS har mulighet til å gjøre forbedringer i internkontrollen, og at mulige brudd på policy, regelverk eller retningslinjer rapporteres til ansvarlig person. På denne måten kan Eid Elektro AS lære av avvik, og iverksette tiltak for å forbedre systemet. Avvik i forhold til behandling av personopplysninger registreres som avvik i bedriftens avvikssystem.

Bedriften skal iverksette tiltak dersom:

- Personopplysninger behandles i strid med fastlagte rutiner
- Det er mistanke om eller dokumentert brudd på informasjonssikkerhet
- Dersom uautorisert utlevering av personopplysninger har funnet sted.

Dersom det har skjedd en uautorisert utlevering av personopplysninger skal den berørte varsles når det er sannsynlig at avviket vil medføre høy risiko for personvernet til den som er berørt. Det må også vurderes om Datatilsynet skal varsles om avviket.

Følgende rutiner er etablert i denne prosedyren:

1. Rett til innsyn, GDPR art. 15
2. Innsamling av personopplysninger, GDPR art. 13.
3. Retting av personopplysninger, GDPR art. 16

4. Sletting/anonymisering av personopplysninger, GDPR. Art. 17.
5. Rutine for arbeidsgivers innsyn i e-post mv., personopplysningsforskriften § 9-3.
6. Særlig om sensitive personopplysninger for ansatte (fagforeningstrekk og sykemeldte arbeidstakere)
7. Rett til dataportabilitet, GDPR. Art. 20
8. Kameraovervåking (se prosedyre “00.111 Kameraovervåkning og tilgangskontroll i egen bedrift”)
9. IT-sikkerhet og informasjonssikkerhet, se egen beskrivelse i bedriften.
10. Elektronisk kjørebok (se prosedyre 20.008 Elektronisk kjørebok og flåtestyring)
11. Adgangskontroll (se prosedyre 00.111 Kameraovervåkning og tilgangskontroll i egen bedrift)
12. Tids- og ordreregistrering, se egen beskrivelse i bedriften.
13. Databehandleravtaler

Rett til innsyn En henvendelse fra en registrert person skal behandles så raskt som mulig og senest innen 10 arbeidsdager, med mindre særlige forhold gjør at lengre tid er påkrevet. Retten til innsyn omfatter ikke opplysninger som:

- Det må anses utilrådelig at den registrerte får kjennskap til, av hensyn til vedkommendes helse eller forholdet til personer som står vedkommende nær.
- Det utelukkende finnes i tekst som er utarbeidet for den interne saksforberedelse og som heller ikke er utlevert til andre i medhold av lov gjelder taushetsplikt for.
- Det vil være i strid med åpenbare og grunnleggende private eller offentlige interesser å informere om, herunder hensynet til den registrerte selv.

Eid Elektro AS kan i utgangspunktet selv velge hvordan informasjonen skal gis, med mindre det stilles krav om en skriftlig redegjørelse. Daglig leder/de respektive

seksjonsledere/avdelingsleder e.l. har ansvaret for at informasjonsplikten blir oppfylt innenfor eget ansvarsområde. HR/Personalseksjonen/adm. leder e.l. er ansvarlig for å gi informasjon om innsamling av personopplysninger om egne ansatte.

Lagring av personopplysninger Det er viktig at oppbevaring og lagring av personopplysninger skjer i tråd med personopplysningsloven § 13 som sier at det skal sørges for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet.

Videre sier GDPR art. 5 f) at *"personopplysninger skal 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 fortrolighet»)."*

Dette betyr at ved lagring av personopplysninger i Eid Elektro AS skal det sikres at:

- Uvedkommende ikke får tilgang til opplysningene.
- Informasjonen skal ikke kunne endres under lagring uten at det er gyldig grunnlag for dette.
- Informasjonen må være tilgjengelig for de som har behov for den i sin jobbutførelse.

Bedriften må selv avgjøre om det er nødvendige å beskrive nærmere om de organisatoriske og tekniske tiltak samt de systemene som benyttes for de respektive behandlingene av personopplysninger.

Rettingen av opplysninger Rettingen av opplysninger skal omfatte både opplysninger som er uriktige og opplysninger som er ufullstendige. Retting av opplysninger skal skje etter eget tiltak dersom feil oppdages eller i etterkant av en konkret henvendelse med anmodning om slik retting. Det kan bes om at

den registrerte bidrar til å informere dersom opplysningene er mangelfulle eller feilaktige.

Sletting av ansattes personopplysninger Personopplysninger om egne ansatte i Eid Elektro AS skal som hovedregel lagres frem til arbeidsforholdet er formelt avsluttet og Eid Elektro AS ikke lenger har behov for opplysningene.

Stilling/avdeling i Eid Elektro AS har ansvar for å gjennomføre sletting. Dersom opplysninger er av en slik karakter at de ikke kan slettes, skal de i størst mulig grad anonymiseres.

Eid Elektro AS kan for alltid oppbevare informasjon om arbeidstakers navn, ansettelsesperiode og stilling i Eid Elektro AS.

Sletting av privatkunderegister Personopplysninger i kunderegister skal oppbevares i minst 5 år etter reklamasjonsreglene i forbrukerlovgivning og i 10 år etter bokføringslov. Det kan også være behov for lengre oppbevaring for å dokumentere valgte løsninger i systemer mv.

Som hovedregel har Eid Elektro AS kommet til at opplysningene i kunderegister ikke skal slettes. Personopplysningene i registeret er vurdert å ha tilnærmet ingen risiko for krenkelse av personvern, og opplysningene anses som godt sikret i oppbevaringsmedium. Opplysningene vil imidlertid bli slettet ved krav/henvendelse fra registrert person.

Rutine for arbeidsgivers innsyn i e-post mv., personopplysningsforskriften § 9-3. I henhold til personopplysningsforskriften § 9-2 har arbeidsgiver bare rett til å gjennomsøke, åpne eller lese e-post i arbeidstakers e-postkasse, elektroniske filer mv. i særskilte tilfeller. I Eid Elektro AS anses følgende tilfeller for saklig grunnlag for arbeidsgivers adgang til innsyn:

- Nødvendig systemadministrasjon for å sikre etterlevelse av

krav i avtaler eller policy for informasjonssikkerhet. Eksempler på dette kan være søk etter ødeleggende data som f.eks. virus og trojanere, eller ved begrunnet mistanke om arbeidstakers sending av ødeleggende data.
- Ved begrunnet mistanke om straffbare forhold.
- Behov for tilgang til den ansattes data ved fravær, for å kunne gjennomføre virksomhetsrelaterte oppgaver eller når det er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten.
- Ved begrunnet mistanke om at arbeidstakers bruk av e-postkassen medfører grovt brudd på de plikter som følger av arbeidsforholdet, eller som kan gi grunnlag for oppsigelse eller avskjed.

Eid Elektro AS prosedyre ved innsyn er basert på reglene i personopplysningsforskriften § 9-3:

1. Arbeidstaker skal varsles på forhånd i den grad dette er mulig. Etter en vurdering kan dette avvikes for særskilte forhold, f.eks. ved en etterforskning av lovbrudd eller dersom det ikke er tid til dette for å kunne gjennomføre virksomhetskritiske oppgaver.
2. Arbeidstaker skal som hovedregel være til stede ved innsynet, og har rett til å la seg bistå av tillitsvalgt eller annen representant.
3. Innsyn i informasjon merket “privat” skal unngås dersom dette er mulig.
4. Dersom arbeidstaker ikke var til stede, skal arbeidstaker varsles skriftlig så snart det lar seg gjøre etter at innsynet er gjennomført. Dersom særskilte hensyn, f.eks. pågående etterforskning, gjør at dette ikke er ønskelig, kan kravet om varsling avvikes. Avviket skal dokumenteres.

Særlig om sensitive personopplysninger for ansatte Eid Elektro AS vil i varierende grad være pålagt å behandle to kategorier sensitive personopplysninger om våre ansatte. Dette

vil være informasjon om fagforeningsmedlemskap og arbeidstakeres helseforhold.

Eid Elektro AS har tariffavtalefestet plikt til å forestå trekk av fagforeningskontingent for arbeidstakere som er medlemmer av fagforbund. Dette er informasjon som den ansatte enten gir selv eller som blir sendt oss direkte fra den respektive arbeidstakerforening.

Videre har vi lovfestet plikt etter arbeidsmiljøloven og folketrygdloven til å behandle opplysninger om arbeidstakeres helseforhold ved sykemeldinger/oppfølgning av sykemeldte arbeidstakere.

Opplysninger om ansattes fagforeningsmedlemskap skal kun behandles av de representanter for bedriften som har behov for denne informasjon. Angi funksjon, f.eks. lønningskontor, administrativ stilling/funksjon e.l.

Opplysninger om ansattes helseforhold skal begrenses til de administrative funksjoner som ivaretar arbeidsgivers forpliktelser etter loven. Det er kun disse ansatte som skal ha tilgang til opplysningene. Angi funksjon, f.eks. lønningskontor, administrativ stilling/funksjon e.l.

Det bør gis en kort beskrivelse av hvem som skal ha tilgang til disse opplysningene, hvorfor disse må ha tilgang, og en angivelse av hvordan opplysningene lagres.

Rett til dataportabilitet, GDPR. Art. 20 Den registrerte skal ha rett til å motta personopplysninger om seg selv som vedkommende har gitt til en behandlingsansvarlig. Dersom Eid Elektro AS mottar en henvendelse etter denne bestemmelsen, skal denne etterkommes så snart som mulig og innen 10 virkedager av stilling/funksjon/avdeling e.l.

Kameraovervåking, jf. personopplysningsforskriften § 8-4 Med kameraovervåking menes vedvarende eller regelmessig

gjentatt personovervåking ved hjelp av en fjernbetjent eller automatisk virkende fjernsyn eller videokamera, fotografiapparat e.l.

Kameraovervåkingssystemene har som formål å hindre at uvedkommende skaffer seg adgang til Eid Elektro AS sine arealer og skal virke preventivt på uønsket adferd som innbrudd, tyveri, hærverk mv. (evt. annet formål)

I henhold til personopplysningsforskriften § 8-4 skal opptak slettes når det ikke lenger er saklig grunn for oppbevaring og senest innen 7 dager etter opptakene er gjort. Områder som overvåkes skal tydelig merkes.

Ansvar for oppfølgning av denne rutinen ligger hos Kjøllesdal Ove. Internkontrollsystemet skal også inneholde følgende:

- Beskrivelse av IT-sikkerhet og informasjonssikkerhet. Dette bør ivaretas av IT-sjef eller annen lignende funksjon.
- Elektronisk kjørebok: Beskrivelse av system og evt. annen dokumentasjon, avtale med tillitsvalgte eller ansatte, mv.
- Adgangskontroll Beskrivelse av system og evt. annen dokumentasjon, avtale med tillitsvalgte eller ansatte, mv.
- Tids- og ordreregistrering Beskrivelse av system og evt. annen dokumentasjon, avtale med tillitsvalgte eller ansatte, mv.

Databehandleravtaler Hvis en virksomhet setter ut hele eller deler av behandlingen av personopplysninger til andre virksomheter, er den eller de som behandler opplysningene definert som databehandlere. En databehandler kan ikke behandle personopplysninger på en annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Den behandlingsansvarlige skal forsikre seg om at databehandleren har tilstrekkelig sikkerhetsnivå, jf. personopplysningsloven § 15 og GDPR art. 28.

Denne opplistingen er ikke fullstendig og bedriften må selv

besørge at alle behandlinger av personopplysninger er omtalt i dokumentet.

Henvisning

Databehandleravtaler mellom Eid Elektro AS og datterselskap

Personopplysningsloven

Personopplysningsforskriften som lovfester hvordan personopplysninger behandles som helt eller delvis skjer med elektroniske hjelpemidler

Aktive oppgaver