

Personvern: Avvikshåndtering

Avvikshåndtering – håndtering av avvik ved behandling av personopplysninger

1. Innledning

Personopplysningsloven og personopplysningsforskriften setter krav til behandling av personopplysninger. Epleskogen barnehage SA skal behandle personopplysninger i tråd med personopplysningsloven og personopplysningsforskriften. Under utføring av barnehagens oppgaver skal personvernet ivaretas på en god måte. Dette dokumentet beskriver barnehagens rutiner for avvikshåndtering ved behandling av personopplysninger.

Hovedregelen er at alle avvik som skyldes brudd på datasikkerheten skal meldes til Datatilsynet. Unntak fra dette gjelder hvis det er usannsynlig at avviket medfører en risiko for enkeltpersoners rettigheter eller personvern.

Det stilles samtidig krav til at avviksmeldingen skal leveres til Datatilsynet innen 72 timer. Dersom barnehagen ikke har full oversikt over avviket, kan den sende avviksmeldingen trinnvis.

Barnehagen må ha dokumentasjon på alle avvik og hvilke tiltak som er iverksatt. Formålet med avviksmeldingen er at Datatilsynet skal kunne kontrollere at reglene om avviksvarsling følges.

1.1 Hva er personopplysninger

Personopplysninger innebærer alle opplysninger som kan knyttes til en enkeltperson, f.eks. navn, fødselsnummer, adresse, telefonnummer, bilder og kommunikasjon mellom foreldre og barnehagen. Sensitive personopplysninger kan være opplysninger om rasemessige bakgrunn, politisk og religiøs oppfatning, tidligere straffeforhold eller at en person har vært mistenkt, siktet eller tiltalt for straffbare handlinger, helseforhold, seksuelle forhold og medlemskap i fagforeninger.

1.2 Eksempler på avvik

En uautorisert utlevering av personopplysninger er når personopplysninger befinner seg utenfor den behandlingsansvarliges kontroll, og personer som ikke er godkjent for tilgang til personopplysningene kan ha fått tilgang. En utlevering kan være tilsiktet eller utilsiktet. Det har skjedd en utlevering selv om det er usikkert om noen har fått personopplysningene i hende.

1.2.2 Eksempler på uautorisert utlevering

Forsendelsesfeil

1. Personopplysninger er sendt til feil mottaker pr. post eller e-post.
2. Digitale forsendelser som avslører andres e-postadresse i en kontekst hvor mottakerne skal beskyttes.
3. Forsendelser til riktig mottaker, men som ved en feil også inneholder personopplysninger om andre.

4. Postforsendelser til riktig mottaker, men hvor det er informasjon om mottakeren som skal skjermes for andre er synlig utenpå forsendelsen. Eksempler på dette er synlig fødselsnummer.

5. Postforsendelser hvor innholdet mangler eller innholdet er der, men konvolutten er revet opp.

Hacking eller datainnbrudd, hvor personopplysninger har blitt hentet ut eller at det er sannsynlig at dette har skjedd.

Snoking gjennomført av egne ansatte. Dette er en utlevering fordi ansatte har ervervet opplysningene til sine private formål, og arbeidsgiver har derfor tapt kontrollen med opplysningene.

Tilgangsstyring feilet, er mangelfull eller manglende, slik at uvedkommende fra utsiden av virksomheten har fått tilgang til beskyttelsesverdige personopplysninger.

Nettpublisering av personopplysninger som ikke skulle ha vært publisert, eller at personopplysningene ikke har blitt anonymisert.

Fysisk innbrudd hvor digitale data eller papirdokumenter med personopplysninger er forsvunnet.

Avhending uten sletting eller makulering

Mistet/gjenglemt/forlagt:

Papirdokumenter, Laptop, nettbrett eller telefoner der innholdet ikke er kryptert. Minnepinner eller andre små lagringsmedier der innholdet ikke er kryptert.

2. Formål

Ansatte i barnehagen har kjennskap til hvordan de skal håndtere avvik ved behandling av personopplysninger. Rutinen skal avdekke og forbedre forhold som ikke tilfredstiller kravene til personvern.

3. Handling

Enhver som behandler personopplysninger på vegne av Epleskogen barnehage SA skal ved mistanke om at personopplysninger har kommet på avveie melde ifra om dette til daglig leder.

Daglig leder vil vurdere hendelsen og eventuelt kontakte Datatilsynet og holde Eierstyret informert.

Når et avvik er oppdaget skal oppfølgingen loggføres fortløpende i eget skjema for håndtering av avvik (vedlegg) og saken håndteres som følger:

A) Kartlegg hvilke opplysninger som har vært tilgjengelige for hvem.

Det skal kartlegges hvilke typer opplysninger avviket dreier seg om, hvem de registrerte er samt hvor opplysningene stammer fra.

B) Gjennomføre skadebegrensende tiltak

Det skal straks gjennomføres nødvendige skadebegrensende tiltak. Dette kan f.eks. bestå av å fjerne tilgang til dokumenter og informasjon, korrigere mangelfulle eller gale opplysninger, orientere mottakere av slik informasjon om mangelen.

C) Fjerne tilgang for gjeldende dokument/tjeneste Uberettiget tilgang til opplysningene skal fjernes. Opplysninger det ikke er behov for, eller kopier av slike, være deg seg fysiske eller digitale, skal slettes.

D) Informasjon til de registrerte Den eller de registrerte som avviket gjelder skal normalt varsles om hendelsen.

E) Dokumentere avviket og utarbeide rapport Etter hendelsen skal barnehagen skrive rapport som dokumenterer hva som har skjedd og hvilke tiltak som er gjort. Daglig leder vurderer også om rapporten skal sendes Datatilsynet samt om hendelsen skal informeres internt til ansatte.

Avviksrapporten skal inneholde:

- en beskrivelse av avviket, hva slags personer og personopplysninger som er berørt.
- et anslag på hvor mange personer og oppføringer av personopplysninger som er berørt av sikkerhetsbruddet ☐
- kontaktinformasjon til personvernombudet eller et annet kontaktpunkt i virksomheten ☐
- en beskrivelse av hvilke konsekvenser avviket trolig vil ha ☐
- en beskrivelse av de tiltak som er (planlagt) iverksatt for å lukke avviket og begrense konsekvensene av det

Vedlegg: Skjema for håndtering av avvik

AVVIKSSKJEMA – BEHANDLING AV PERSONOPPLYSNINGER

Fra: (Avdeling og ansatt) Til: Daglig leder Epleskogen barnehage SA

Hva gjelder avviket?

Beskriv avviket: (Hva slags personer og personopplysninger er berørt, hvor mange personer er berørt?)

Hvilke typer personopplysninger har vært tilgjengelig for hvem?:

Hvilke konsekvenser har avviket?

Hvilke eventuelle tiltak er gjennomført og hvilke eventuelle forslag til tiltak har du til hva som kan gjøres for å rette på dette?

Informasjon: Har de berørte personene blitt informert om avviket?

Tidspunkter: Avviket oppdaget: (dato og klokkeslett) Når oppstod avviket?: Angi om mulig når avviket oppstod.