VEILEDER

GDPR – PERSONVERN

DEL 2 - personopplysninger utover ansatteforhold

Nye krav fra 20. juli 2018

Forordningen ble norsk lov og den gjeldende loven ble erstattet. Det nye lovverket styrker forbrukernes rettigheter og virksomhetens plikter. Loven gelder for alle som behandler personopplysninger.

Prinsipper i behandling av personopplysninger

Utgangspunktet i det nye regelverket er at alle har rett til å bestemme over opplysninger om seg selv.

Det betyr at vi, som frivillige organisasjoner, må være bevisste på flere forhold i den daglige driften:

- Lovlig, rettferdig og gjennomsiktig
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet, konfidensialitet og tilgjengelighet
- Ansvarlighet

Våre forpliktelser er å sørge for at vi etterlever lovens krav, sørge for at medlemmer, samarbeidspartnere og offentlige myndigheter kan ha tillit til oss og å gjennom organisasjonens praksis og rutiner knyttet til personopplysninger.

Hva er relevant for oss?

- Alle skal kunne oppfylle nye rettigheter, for eksempel retten til å bli glemt
- Alle skal ha forståelig personvernerklæring
- Alle skal vurdere risiko og personvernkonsekvenser
- Alle skal bygge personvern inn i nye løsninger
- Databehandlerne får nye plikter
- Vi må rapportere til Datatilsynet ved avvikshåndtering

Hva er en personopplysning

Alle opplysninger som kan knyttes til en fysisk person er en personopplysning; navn, fødselsnummer, kontaktinformasjon – postadresse, telefonnummer og epostadresse, bilde, lønnsopplysninger, helseopplysninger, politisk- og religiøs tilhørighet, straff og soning mv.

Begreper i det nye lovverket:
Behandling – innsamling, registrering, sammenstilling, lagring og utlevering
Register – medlemsregister, deltagerlister, ansattelister, bildedatabase, pårørenderegister etc
Behandlingsansvarlig – den som bestemmer formålet med behandlingen og hvordan behandlingen skal gjøres – frivillige organisasjoner, offentlige etater og bedrifter.
Databehandler – den som behandler personopplysninger på vegne av den behandlingsansvarlige – IT-leverandør, Google, Microsoft, Questback, Dropbox, regnskapsfører, fakturaprogram etc.

Frivillige organisasjoners behandling av personopplysninger

Alle frivillige organisasjoner er behandlingsansvarlige og mange kan ha tilgang til informasjonene – ansatte, tillitsvalgte, medlemmer og frivillige. Personopplysninger finnes mange ulike steder – medlemssystem, epost, skyløsninger, digitalt arkiv, papirarkiv, lokalt på egen PC mv. Det er viktig å være bevisst på det nye ansvaret, hva som blir lagret hvor og hvem som har tilgang, samt å innarbeide gode rutiner.

Generell informasjonssikkerhet (rutiner og kvalitet) er sentralt i vår behandling av personopplysninger.

- Hvordan sikrer vi alle persondata – digitalt og fysisk?
- Har vi gode rutiner for informasjonssikkerhet?
- Utarbeide risikovurdering rundt de enkelte persondataene
- Har vi gode og sikre passord?
- Har vi god adgangskontroll – hvem har og må ha tilgang til hva?

Det nye lovverket krever at det foreligger et behandlingsgrunnlag. Det er flere grunnlag for vår behandling av personopplysninger. Det kan være snakk om å oppfylle avtale om medlemskap, oppfylle arbeidsavtalen og samtykkeerklæringen.

I daglig virke er det mye bruk av bilder og film i kommunikasjonen, informasjonen, tagging, rapporteringen mv. Det er særskilte regler for bruk av bilder, bla er det krav om samtykke til å publisere bilder. Dersom bilder tatt på møter skal publiseres, kan det være fornuftig å innhente samtykke ved deltagerregistrering. Det er spesielle hensyn knyttet til publisering av bilder med barn. Ungdom over 15 år kan gi samtykke selv. Unntaksbestemmelse i Åndsverkloven § 45 c:

- Avbildingen har aktuell og allmenn interesse
- Avbildingen er mindre viktig enn hovedinnholdet i bildet
- Bildet gjengir forsamlinger, folketog i friluft eller hendelser som har allmenn interesse

Kom i gang!

(1) Lag en oversikt over alle persondataene dere behandler, hvem som behandler dem og hvor de lagres/oppbevares.
(2) Dokumenter formålet med å oppbevare personopplysninger.
(3) Skriv ned og dokumenter rutinene deres.
(4) Slett alle personopplysninger dere ikke trenger.
(5) Lag samlelister for epost-utsendinger og bruk blindkopi-funksjonen.
(6) Lag rutiner for å innhente samtykke for de persondataene dere behandler.
(7) Lag en personvernerklæring som ligger lett tilgjengelig på nettsiden.
(8) Sørg for oppdaterte avtaler med databehandlerne dere bruker (leverandører av programvare).
(9) Lag en årsplan for gjennomgang av rutiner og risikovurdering av arbeidet med personopplysninger.

Forslag til skjema for bruk i kartleggingsarbeidet:

Kartlegging og gjennomgang av personopplysninger i organisasjonen

Person-opplysninger	Sensistive opplysninger	Formål og grunnlag for behandling	Lagring	Sikkerhetstiltak	Behandlings-ansvarlige	Data-behandlere	Ut-levering	Risikovurdering
Medlemmer: Navn, addresse, e-post, tlf, kontaktperson	Nei		Medlemsregister	• Passord • Rolletildeling • Tilgangskontroll	• Ansatte • Enkelte tillitsvalgte	- Unicornis		
Ansatte: Navn, adresse, e-post, personnumme, bankkonto, pårørendeopplysninger, referat fra medarbeider-samtaler	Ja	• Oppfylle arbeidsavtale • Oppfylle rettslige forpliktelser som arbeidsgiver	• Egen server • Ekstern server • Nettsky • Fysisk mappe	• Taushetserklæring • Innlåste lister • Kode på kopimaskin • Passord	- Leiransvarlig + frivillige	• Outsourcing av HR-funksjon - IT-leverandør		
Forvaltnings-oppgaver: Navn, addresse, e-post, tlf, kontaktperson, historikk								
Nyhetsbrev: • **Navn** • **E-post adresse**	Nei	• Markedsføring. • Oppfylle avtale om medlemskap • Samtykke				- Mailchimp		
Arrangements-deltagere: Navn, addresse, e-post, tlf, kontaktperson, allergier, særskilte behov								

Datasikkerhet på kontoret

Tips for å unngå at personopplysninger (og også andre opplysninger) kommer på avveie:

- Bruk sterke passord og ha rutiner for å endre passord
- Logg ut når du går for dagen
- Ikke lagre sensitive personopplysninger lokalt på PC, minnepinne eller mobil
- Ikke send personopplysninger og sensitive opplysninger på epost – kodes
- Ikke send lister med personopplysninger på epost – kodes
- Slett ”søppelkassen” med jevne mellomrom

Samtykkeerklæring

Det nye lovverket krever at det gis samtykke til behandling av personopplysninger dersom behandlingsgrunnlaget ikke er gitt i annet grunnlag. Tidligere kunne man reservere seg fra at personopplysninger som for eksempel telefonnummer ble lagret.

Samtykkeerklæring er aktuelt for frivillige organisasjoner når det gjelder ansatte- og tillitsvalgte-opplysninger, medlemsopplysninger, mottakere av nyhetsbrev og forvaltning av tilskudd.

En samtykkeerklæring er en frivillig, spesifikk og utvetydig erklæring om at personen aksepterer behandlingen. Det det blir gitt samtykke til skal være forståelig. Et gitt samtykke kan alltid trekkes tilbake.

Vi må ha rutiner for å innhente samtykke og for å slette opplysninger dersom samtykket trekkes tilbake.

Eksempel på samtykkeerklæring:
"Tilskuddsordningen registrerer og lagrer noen personopplysninger om deg når du oppretter profil og søker om midler. Noen opplysninger må vi oppbevare en stund, mens andre sletter vi så fort vi kan. Les om hvilke opplysninger vi oppbevarer og hvordan vi oppbevarer dem i personvernerklæringen (lenke til nettsiden)."

Norsk musikkråd og Musikkens studieforbund arbeider med tekst til samtykkeerklæring og personvernerklæring.

Sletting av personopplysninger

Det er viktig å være klar over at alle personopplysninger man ikke bruker skal slettes. Her er det også nødvendig å se til både bokføringslovens og regnskapslovens bestemmelser, i tillegg til arkivloven. Dersom det er nødvendig å oppbevare personopplysninger som ikke lenger brukes, skal det foretas en nødvendighetsvurdering. Denne vurderingen bør dokumenteres skriftlig. Oppbevaring av medlemsopplysninger for kontroll kan inngå i en slik vurdering.

Det er mulig å oppbevare anonymiserte data. Slik anonymisering kan være "sladding".

Alle har rett til å bli slettet om de selv ønsker det. Det betyr at dersom noen gir beskjed om at vedkommende ikke ønsker å stå som mottaker på et nyhetsbrev eller motta informasjon, skal vedkommende fjernes fra listen.

Risikovurdering, rutinegjennomgang og avviksrapportering

Risikovurdering

Alle som håndterer personopplysninger skal foreta risikovurdering. Det er viktig å være bevisst på hva som kan gå galt og hvor det kan gå galt.

En risikovurdering er et verktøy for å identifisere uønskede hendelser og risikoen for at disse skal inntreffe. Det skal være tilstrekkelig å ha gjort en vurdering av hva som kan føre til avvik og hvilke tiltak som da vil iverksettes.

Som en del av internkontrollen skal vi ha en oversikt over hvilke behandlinger av personopplysninger som foretas, og hvilke personopplysninger som inngår i disse. Denne oversikten skal brukes som underlag ved risikovurderinger.

Vi er forpliktet til å gjennomføre risikovurdering før vi iverksetter en behandling og før man tar i bruk et informasjonssystem.

Rutinegjennomgang

For å ivareta bestemmelsene i og våre forpliktelser etter den nye loven, må rutiner innarbeides i den daglige driften.

Noen rutiner må innarbeides med en gang, noen kan gjøres fortløpende eller med en viss hyppighet.

Eksempel på tidshjul for når man gjør hva:
Nå og senere fortløpende – innhente samtykke for nyhetsbrev og informasjon, utarbeide samtykkeerklæringer for tilskuddsordninger.

Fortløpende – etter valg av tillitsvalgte, nyansettelser informere om oppbevaring av personopplysninger, slette personer dersom de ønsker å bli slettet, rapportere eventuelle avvik.

Ukentlig – gjennomgå sjekklisten og ha GDPR som fast punkt på kontormøtet og slette personopplysninger fra PCen.

Månedlig – øvrige sletterutiner og endring av passord.

Årlig – rutinegjennomgang og foreta risikovurdering.

Avviksrapportering
Det nye lovverket har nytt og strengere krav for rapportering av avvik. Avvik fra rutiner skal meldes til Datatilsynet innen 72 timer. Berørte skal varsles dersom avviket vil medføre høy risiko for personvernet. Dersom varslingsplikten ikke ivaretas, kan Datatilsynet ilegge bøter.

Kilder:
www.datatilsynet.no
www.frivillighetnorge.no