I 2018 innføres ny personvernlovgivning i Norge og Europa. Hva blir annerledes?

I 2016 vedtok EU ny personvernforordning, General Data Protection Regulation (EU GDPR), for å sikre like regler for personvern for alle virksomheter og aktører som opererer i EU- og EØS-land. Med virkning fra 25.mai innføres GDPR som norsk lov, og kommer til å påvirke alle bransjer, virksomheter og organisasjoner.

Gjelder for større geografisk område

Behandlingsansvarlige som er registrert utenfor EU, men som tilbyr varer og tjenester til EU-borgere, vil bli omfattet av det nye regelverket. Det er de ikke i dag. Det gjelder for eksempel nettbutikker som ikke er etablert i Europa, men som selger varer over nett, og kanskje tilbyr frakt til europeiske land og betaling i norske kroner. Regelverket vil også gjelde behandlingsansvarlige som er etablert i tredjeland, men som overvåker adferden til EU-borgere innenfor EU, for eksempel amerikanske selskaper som profilerer EU-borgere på bakgrunn av nettbruken deres.

Hva betyr dette for NMF?

Ingen endring fra dagens praksis.

Opplysninger skal ikke brukes til nye, uforenlige formål

Personopplysninger skal kun behandles der det finnes et tydelig spesifisert formål. Dersom man ønsker å behandle personopplysninger til andre formål enn de var innhentet for, må man forsikre seg om at det nye formålet er forenlig med det gamle. Det som er nytt med det nye regelverket, er at behandlingsansvarlig får hjelp til å avgjøre hva som er forenlige formål og ikke, ved en «kompatibilitets-test» i forordningsteksten. Dersom konklusjonen er at det nye formålet er uforenlig med det gamle, skal det innhentes samtykke, eller behandlingen må hjemles i lov.

Hva betyr dette for NMF?

Innskjerping av hva persondata kan brukes til, men fortsatt åpent for å innhente de data som er nødvendige for å administrere et korps, samtidig som dokumentasjonskravet fra myndighetene ivaretas. Nødvendige data defineres som navn, fødselsdato, kjønn, adresse, e-post og telefon. Dette gjelder også dersom korpset har valgt å registrere foresatte for medlemmer under 18 år.

Merk at samtykke MÅ innhentes dersom data skal brukes til andre formål eller det innhentes sensitive data.

Nye rettigheter for borgere

Forordningen fører med seg fire nye rettigheter for EU-borgere og nordmenn:

Rettigheten til å få behandlingen begrenset, retten til dataportabilitet, retten til å motsette seg en behandling, og rettigheter til å motsette seg profilering og automatiserte avgjørelser.

Du får rett til å motsette deg profilering begått av offentlige myndigheter, og til å motsette deg profilering for direkte markedsføring. Du får også rett til å klage på automatiserte avgjørelser som tas på bakgrunn av en profil som er utarbeidet om deg. Profiler skal ikke utarbeides på bakgrunn av sensitive opplysninger, hvis ikke den registrerte har samtykket eller slik profilering kan begrunnes med en særlig samfunnsinteresse som er hjemlet i lov.

Hva betyr dette for NMF?
Ingen endring fra dagens praksis, data blir ikke delt, og skal heller ikke deles med kommersielle interesser

Bedrifter får større ansvar for personvern

Virksomheter får utvidet sin plikt til å selv vurdere personvernkonsekvenser ved behandling av personopplysninger. Denne plikten utvides, og det ser ut til at færre vil trenge å søke konsesjon fra sitt lands personvernmyndigheter, som Datatilsynet i Norge. De får også plikt til å identifisere risikoreduserende tiltak. Kun i de tilfellene der risikoen ikke kan håndteres på en tilfredsstillende måte internt, skal de søke forhåndsgodkjenning fra nasjonale myndigheter (Datatilsynet). Innebygd personvern og personvern som standardinnstilling i applikasjoner blir lovpålagt.

Hva betyr dette for NMF?
I første rekke at alle ansatte og tillitsvalgt må sette seg inn i hvilke regler som gjelder, og påse at persondata kun brukes til formålet. Persondata vil fortsatt kunne samles inn for å kunne administrere korpset, samt ivareta dokumentasjonskravet fra myndighetene.
Merk også at eventuelle medlemmer/foresatte med hemmelig adresse IKKE skal kunne identifiseres via korpsets registrerte persondata.

Personvernombudet blir mer sentralt enn tidligere

Det vil høyst sannsynlig bli flere *personvernombud*, fordi flere virksomheter enn i dag vil plikte å opprette ombud. Disse vil trenge *personvernombud*:

1. Offentlige virksomheter
2. Virksomheter som behandler sensitive personopplysninger i stor skala
3. Virksomheter som systematisk overvåker europeiske borgere i stor skala

Norge kan også pålegge andre å ha *personvernombud* gjennom lovregulering. I store trekk blir oppgavene og forventningene til *personvernombud* uendret. Det presiseres i forordningsteksten at det er viktig at ombudene unngår interessekonflikt, og det kommer et eksplisitt krav om at bedriften skal legge til rette for at personvernombudene skal kunne få tid og rom til å gjøre en god jobb.

Databehandlere skal på lik linje med behandlingsansvarlige oppnevne *personvernombud*. De skal sørge for *informasjonssikkerhet* og dokumentere det, gjennomføre risikovurderinger. Innholdskravene til en *databehandleravtale* er gitt i forordningen. Slik var det ikke tidligere.

Hva betyr dette for NMF?
I utgangspunktet ingen endring fra dagens praksis. Det vurderes fortløpende om NMF skal opprette et eget personvernombud, men siden NMF ikke inngår i noen av de tre punktene nevnt over, avventes dette.

Et klart språk og krav til åpenhet

Det er et viktig prinsipp i forordningen at informasjon om behandling av personopplysninger skal gis på en klar og tydelig måte, og ikke gjemmes bort i en personvernerklæring. Det kan se ut til at den registrerte har fått styrket sitt krav på åpenhet. Det er et viktig prinsipp at behandlingen for de registrerte skal fremstå som åpen og rimelig. Opplysningene om hvilke registreringer som gjøres, skal gis på en klar og tydelig måte, i lett forståelig språk. Informasjonen skal gis uten vederlag. Behandlingsansvarlige får på sin side en plikt til forsikre seg om at de henvender seg til rette vedkommende når de for eksempel gir elektronisk informasjon om behandlingene.

Hva betyr dette for NMF?

Samtlige medlemmer har til enhver tid tilgang til de data som er registrert i NMFs systemer via pålogging til 'MIN SIDE' (https://musikkorps.no/login/ der brukernavn = medlemsnr. Ved innmelding i korps sendes det ut velkomstmelding med informasjon om dette til det nye medlemmet. For eksisterende medlemmer kan korpset selv informere om medlemsnr (står under fanen MEDLEMMER i Korpsdrift, og på korpsets årsrapport), passord hentes via rutinen 'Glemt passord'.
NMFs personvernerklæring finnes på www.musikkorps og på 'Min side'.

Plikter å samarbeide internasjonalt

Nasjonale datatilsyn får en plikt til å samarbeide og utveksle informasjon med hverandre. Samarbeidet skal inkludere utveksling av informasjon i konkrete saker.

Datatilsynet skal opptre uavhengig i Norge, men samtidig være del av et europeisk felleskap. I store europeiske saker skal konsistensmekanismen anvendes: Datatilsynsmyndighetene i alle landene som er berørt av saken, plikter å samarbeide. Et ledende tilsyn oppnevnes, et tilsyn som skal stå for kontakten med behandlingsansvarlige, registrerte og så videre. Blir ikke de nasjonale myndighetene enige, må saken løftes til European Data Protection Board (EDPB), et nytt EU-organ som er gitt myndighet til å gjøre bindende avgjørelser i konkrete saker i tillegg til å avgi uttalelser om hvordan forordningen skal tolkes.

De nasjonale datatilsynene får videre fullmakter til å ilegge sanksjoner. Etter det nye regelverket kan Datatilsynet gi gebyrer på opptil fire prosent av en virksomhets årlige, globale omsetning.

Hva betyr dette for NMF?

Ingen endring fra dagens praksis.

Hovedelementene i den nye personvernloven (basert på EU-direktivet):

- **Bruk av personopplysninger kun til formålet de er innsamlet i** (artikkel 5).
  Du skal vite klart og tydelig hva dine personopplysninger brukes til, og du har også rett til tilgang til dine personopplysninger.

- **Rett til å bli slettet** (artikkel 17)
  Hvis du ikke lenger er kunde, eller i vårt tilfelle medlem, eller hvis du ikke ønsker at dine personopplysninger skal brukes for eksempel i markedsføring, har du rett til å få slettet dine personopplysninger.

- **Rett til portabilitet** (artikkel 20)
  Du har rett til å overføre opplysninger fra en leverandør til en annen, for eksempel om du skal bytte bank eller forsikring. Dette må skje i maskinlesbart format.

- **Samtykke må gis på en forståelig måte** (artikkel 25)
  Virksomheter kan ikke behandle dine personopplysninger med mindre du har gitt et spesifikt og klart samtykke. Et samtykke må gis aktivt, det blir følgelig slutt på "I agree" etter et uendelig antall sider med liten skrift som du ikke fullt ut forstår.

Hva menes med personlige data?

Personlige data er alle opplysninger som kan knyttes til deg, for eksempel navn, adresse, telefonnummer, e-postadresse, IP-adresse, bilnummer, bilder, fingeravtrykk, irismønster, hodeform (for ansiktsgjenkjenning) og fødselsnummer (både fødselsdato og personnummer).

Hva menes med sensitive data?

Sensitive data er f.eks. rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, livssyn, fagforeningsmedlemskap, genetiske eller biometriske opplysninger, helseopplysninger, seksuelle forhold eller seksuell orientering.

I NMF har vi ikke behov for slike opplysninger, og de skal følgelig ikke innhentes/lagres. Unntak kan gjelde for opplysninger om f.eks. matallergier i forbindelse med korpsturer, sommerkurs o.l., men KUN dersom det innhentes aktivt samtykke fra medlemmet eller dets foresatte. Helseopplysninger skal uansett slettes når formålet med innsamlingen er fullført, f.eks. etter avsluttet sommerkurs.

Retten til å bli glemt

Retten til å bli glemt er primært rettet mot bedrifter som samler inn og sammenstiller data til markedsføringsformål. Retten til å bli glemt medfører at dersom kundene mister tillit, kan de trekke samtykket sitt og da må virksomheten kunne slette opplysninger fra siste back-up til den mest perifere skyleverandør.

NMF selger/utleverer ikke persondata til andre, men respekterer at dersom et medlem slutter, og ønsker å slette alle spor, vil også all informasjon som kan tilbakeføres til et enkeltmedlem slettes. I de tilfeller f.eks. tilskudd er gitt på bakgrunn av medlemskap, eller det er fakturert på et medlem vil data bli beholdt så lenge dokumentasjonskravet fra myndighetene varer, som hovedregel inntil fem år regnet fra 1.januar året etter avsluttet medlemskap.

Hva gjør NMF?

Siste året har NMF brukt på å skaffe oversikt over hvilke persondata som behandles (samles inn, brukes, lagres) og hvor og hvordan disse behandles. Eksterne databehandlere er kontaktet, og nødvendige avtaler skal være signert innen loven trer i kraft. Regelverket er svært omfattende, og det er brukt mye tid på å finne ut hvilke plikter som gjelder NMF. Regelverket er det samme uavhengig av størrelsen på bedriften/organisasjonen, men må tilpasses virksomheten.

Det er brukt mye tid på å bygge kompetanse, avklare roller og ansvar og ikke minst dokumentere rutiner.
Personvernet skal også ivaretas av IT-løsningene. Det vil derfor bli gjennomført en del endringer i Korpsdrift.no/Min Side, i hovedsak:

- Krav om aksept av brukervilkår for tilgang til medlemsdata
- Krav om samtykke via Min Side

Om brukervilkårene ikke aksepteres blir det heller ikke gitt tilgang til Korpsdrift

NMFs personvernerklæring vil bli lagt ut på Korpsdrift.no, Min side og www.musikkorps.no

Mye kan løses datateknisk, men grunnet kravene fra Barne- og likestillingsdepartementet og Norsk musikkråd om å sikre unike medlemskap (ett medlem = ett medlemsnr) må det fortsatt være mulig å søke frem rett person i Korpsdrift, men KUN etter aksept av brukervilkår.

En viktig forutsetning er at det klart fremgår at et medlemskap i et av NMFs medlemskorps innebærer at en del personlig informasjon må oppgis, og hvorfor.
Det er altså frivillig å bli medlem, men dette betinger at nødvendig og korrekt informasjon oppgis ved innmelding.

For enkelte data MÅ det innhentes aktivt samtykke.
Dette gjelder i ALLE tilfeller der sensitiv informasjon innhentes, men kan eventuelt også innhentes dersom behandlingsgrunnlaget for behandlingen er en interesseavveining (dagens personopplysningslov § 8 bokstav f). I NMF vil dette gjelde informasjon som kreves fra myndighetene for å kunne dokumentere medlemskap.
Dersom behandlingsgrunnlaget for behandlingen er samtykke, kan samtykket trekkes tilbake, og en rutine for dette må etableres.

Hva må korpsene gjøre?

Hvert korps vil ha et selvstendig ansvar for hvordan persondata behandles internt i korpset. Merk at dersom korpset benytter andre registreringssystem for medlemmer enn Korpsdrift må det gjøres en egen databehandleravtale med leverandøren av dette.
Mal for databehandleravtale finnes på www.datatilsynet.no.

Som for NMFs ansatte bør korpsene gå gjennom hvilke data som lagres, uavhengig av medium, og hvem som har tilgang til disse. Dette gjelder også data som lagt inn i f.eks. Korpsdrift utover det som er nødvendig for å kunne administrere korpset.
Det bør også innhentes en bekreftelse fra samtlige som har tilgang til persondata om at data skal behandles i henhold til personvernlov. Et eksempel på dette ligger vedlagt.

En kort sjekkliste kan være nyttig å følge:

- Har korpset innhentet sensitiv informasjon, og er det i tilfelle innhentet samtykke til dette?
- Ligger korpset medlemsliste åpent på korpsets nettsider?
- Er det laget interne regler for hvem som skal ha tilgang til persondata, og hvordan disse skal behandles?
- Deles det ut utskrifter av medlemslister, i tilfelle til hvem og hvordan skal disse behandles, også etter bruk?
- Blir persondata delt med eksterne parter?

Hva er konsekvensene av å bryte GDPR?

Siden GDPR-direktivet ble vedtatt i EU har mange, særlig i konsulentbransjen, hengt seg opp i de høye bøtesatsene.
Mange frykter derfor høye bøter dersom den nye personvernforordningen brytes, og man for eksempel ikke sletter personer som ønsker å bli slettet fra et nettsted. Tidligere praksis og informasjon fra datatilsynet tilsier noe annet.
En rapport om virksomheter i 21 europeiske land som hadde brutt personvernlovgivningen, viser at det var få som fikk bøter. I teorien kan man få bøter på opptil 4 % av selskapets globale omsetning, eller inntil 20 millioner Euro, men det er lite sannsynlig at EU vil skyte med de største kanonene på “vanlige virksomheter som gjør så godt de kan”.

I første omgang vil Datatilsynet påpeke feil og mangler, og veilede i prosessen mot full tilpasning til personvernloven.