2018-05-14

FAQ om GDPR

Den 25 maj 2018 börjar EU:s nya dataskyddsförordning att gälla. Den baseras på EU-förordningen *General Data Protection Regulation (GDPR)* och innebär att Personuppgiftslagen (PuL) som gäller idag för behandling av personuppgifter i en verksamhet upphör att gälla.

GDPR lägger stor vikt vid att känsliga personuppgifter ska hanteras med stor aktsamhet och ställer stora krav på hur detta ska ske.

GDPR har skapats för att säkerställa individens rättigheter kring person-uppgifter. Precis som för alla andra organisationer kommer GDPR även att påverka landets alla fackförbund. Medlemskap i ett fackförbund är en känslig personuppgift på samma sätt som etnicitet, sexuell läggning, hälsa eller politisk åskådning.

Vad står förkortningen GDPR för?

GDPR är en förkortning för *General Data Protection Regulation*.

Vad innebär GDPR?

GDPR innebär en reglering för all form av behandling av information som direkt eller indirekt kan knytas till en person. För myndigheter, företag och organisationer kan detta komma att betyda förändringar av hur personuppgifter hanteras.

Dataskyddsförordningen (GDPR) ersätter Personuppgiftslagen (PUL) som infördes 1998 vars syfte var att skydda människor mot att deras personliga integritet kränks när personuppgifter behandlas.

När börjar GDPR att gälla?

GDPR börjar gälla den 25 maj 2018.

Varför införs GDPR?

GDPR införs i syfte att säkerställa individens integritet och för att harmonisera lagstiftning inom EU.

Vad är syftet med GDPR?

Dataskyddsförordningen syftar till att stärka och harmonisera skyddet för levande, fysiska personer inom EU vid hantering av personuppgifter. Förordningen antogs under 2016 och gäller fullt ut från och med den 25 maj 2018. Den ersätter då Dataskyddsdirektivet från 1995.

Till skillnad från ett EU-direktiv kräver en EU-förordning inte att nationella lagar skapas. Den gäller direkt i alla medlemsstater och ersätter då tidigare nationella bestämmelser. Varje enskild medlemsstat har dock rätten att komplettera förordningen med nationella regler i viss omfattning, till exempel hur ett myndighetsbeslut kan överklagas.

Vad är en personuppgift?

En personuppgift är information som direkt eller indirekt går att koppla till en individ. Exempel på sådana är namn eller personnummer men även medlemsnummer, mobilnummer, foton, IP-nummer och e-postadress räknas som personuppgifter.

Vad är känsliga personuppgifter?

Med känsliga personuppgifter avses uppgifter om

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i en fackförening
- hälsa
- en persons sexualliv eller sexuella läggning
- genetiska uppgifter och
- biometriska uppgifter som entydigt identifierar en person.

Genetiska och biometriska uppgifter liksom uppgifter om sexuell läggning är nya kategorier som lagts till som känsliga uppgifter i dataskydds-förordningen jämfört med personuppgiftslagen.

Genetiska uppgifter är personuppgifter som rör en persons nedärvda eller förvärvade genetiska kännetecken, vilka till exempel kan framgå av en dna-analys. Biometriska uppgifter är personuppgifter som rör en persons fysiska, fysiologiska eller beteendemässiga kännetecken som erhållits genom en särskild teknisk behandling, till exempel fingeravtrycksuppgifter.

Vad innebär GDPR för fackliga organisationer?

Medlemskap i ett fackförbund är enligt GDPR en så kallad känslig uppgift. Det ställer därför extra höga krav på ett fackförbund att hantera information rätt. Andra känsliga uppgifter är ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, uppgifter om en fysisk persons sexualliv eller sexuella läggning, uppgifter om hälsa som till exempel kost och allergier.

Vad innebär det att föreningen måste ha en laglig grund för behandling av personuppgifter?

För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett stöd i dataskyddsförordningen, dvs. en laglig grund. De lagliga grunderna är avtal, uppgift av allmänt intresse, intresseavvägning, rättslig förpliktelse, skydd av den registrerades grundläggande intressen, myndighetsutövning och samtycke.

Förutom kravet på rättslig grund måste behandlingen också uppfylla övriga bestämmelser i förordningen. Exempelvis måste föreningen följa de grundläggande principerna och tillvarata individens rättigheter.

Vad är ett personuppgiftsbiträde?

Ett personuppgiftsbiträde är en extern part utanför organisationen som får ta del av information. Exempel på personuppgiftsbiträden kan vara en arbetsgivare som tillhandahåller plats på sina datorer åt föreningen, en IT-leverantör eller ett tryckeri. För att kunna dela information till extern part ska ett personuppgiftsbiträdesavtal upprättas. I ett sådant avtal ska bl.a. anges vad informationen får användas till och hur den ska gallras.

Vad är ett dataskyddsombud?

Enligt GDPR ska organisationer som hanterar känsliga uppgifter i stor skala och som del av sin kärnverksamhet tillsätta ett dataskyddsombud. Eftersom fackförbund i stor skala hanterar känslig information om sina medlemmar är fackförbund enligt GDPR skyldiga att tillsätta dataskyddsombud.

Vilken roll har ett dataskyddsombud?

Ett dataskyddsombud är en person med mycket goda kunskaper om dataskyddslagstiftning och dataskydd. Dataskyddsombudet ska övervaka dataskyddsarbetet inom organisationen och vid behov ange riktlinjer för hur dataskyddsarbetet ska bedrivas. Detta gäller särskilt vid förändringsarbete. Dataskyddsombudet har också en rådgivande funktion inom organisationen.

Är det möjligt att ta emot exempelvis lönelistor från arbetsgivaren?

Om det finns ett specifikt syfte som exempelvis vid en löneöversyn har ni rätt att ta emot lönelistor från arbetsgivaren. Dessa får då användas för att förbereda själva löneöversynen och kontrollera att era medlemmar finns med i underlaget. Efter avslutad lönerevision är det viktigt att listan raderas.

Hur gör jag om jag vill skicka mejl till många samtidigt?

För utskick till flera medlemmar samtidigt, exempelvis en kallelse till föreningens årsmöte eller ett medlemsutskick, ska du alltid skicka via *Hemlig kopia*. Detta för att undvika att alla som får ta del av e-postet ska se vilka det har skickats till. Tänk bara på att i rubriken till utskicket inte ange att mottagaren är medlem i ett förbund.

Kan jag svara arbetsgivaren på om en person är medlem?

Om det finns ett klart syfte kan det finnas laglig grund för att svara på denna fråga. Gäller det exempelvis en fråga där arbetsgivaren vill kalla till förhandling och då behöver veta om ni ska företräda personen har ni rätt att svara på denna fråga. Annars gäller i grunden att ni inte ska svara på om en person har ett fackligt medlemskap.

Har jag möjlighet att berätta om vilka som är medlemmar på en arbetsplats?

Nej, du ska inte berätta för andra om vilka som är medlemmar. Undantag gäller endast förtroendevald på arbetsplatsen.

Hur länge ska dokument sparas i enlighet med den nya dataskyddsförordningen?

Grundregeln är att du bara ska spara information som du behöver för att kunna utföra ditt uppdrag. Arbetsrättsliga ärenden exempelvis tvister där du företrätt medlem ska sparas i tio år enligt preskriptionslagen och ekonomiska dokument ska enligt bokföringslagen sparas i sju år. Gå igenom e-posten och andra ytor där du sparar dokument och radera det som du inte längre behöver.

Hur gör jag med gamla medlemslistor och excel- eller wordfiler som innehåller personuppgifter? Måste dessa raderas?

Listor och dokument som innehåller uppgifter om medlemmar ska raderas så snart som de inte längre är aktuella. Exempel på sådana är exceldokument med uppgifter om medarbetares löner som tagits fram i samband med lönerevisionen. När revisionen är över ska denna raderas.

I syfte att skapa kontinuitet och följa löneutvecklingen på arbetsplatsen kan uppgifterna avidentifieras. Alternativet är att göra en sammanställning utan uppgifter på individnivå.

Vad gäller lagring på exempelvis USB-minne och externa hårddiskar. Omfattas dessa också av bestämmelserna i GDPR?

Ja, samtliga former av elektronisk lagring omfattas.

Hur förvaras och lagras anteckningar och protokoll?
Lagra endast sådan information som är aktuell och som behövs i uppdraget. Lagring får göras i separat mapp i arbetsgivarens nätverk eller inlåst i utskriven form.

Ibland förekommer det att enskilda medlemmar diskuteras vid styrelsemöten. Hur ska protokoll från dessa möten hanteras där enskilda medlemmar nämns.

Närvaro av styrelseledamöter bör kunna skrivas ut i protokoll. I övrigt bör inga personuppgifter nämnas i protokoll som offentliggörs. Om det är tvunget att hänvisa till personer i protokoll, välj istället att döpa dem till Person A, Person B, Person X osv.

Hur får vi förvara listor på medlemmar, exempelvis i samband med lönerevisionen?

Lagra uppgifterna i särskilda mappar med begränsad tillhörighet. Säkerställ att listorna raderas när lönerevisionen är avslutad och de inte längre behövs. Listor och lönestatistik utan information om enskilda medlemmar kan sparas för att exempelvis skapa kontinuitet kring lönerevisionen.

Hur ska exempelvis MBL-protokoll och enskilda förhandlingar hanteras?

Den typen av dokumentation ska sparas i 10 år. Var noga med att lagra dem på en säker plats med begränsad behörighet.

Kan en medlem ta del av ett MBL-protokoll i vilket medlemmen berörs?

Nej, MBL-protokoll får inte lämnas ut när det innehåller personuppgifter på andra än personen själv. Antingen lämnas en muntlig redogörelse för medlemmen av den del i protokollet som medlemmen omfattas alternativt avidentifieras protokollet så att endast personuppgifter från berörd medlem finns med.

Hur ska anmälningslistor till utbildningar och andra aktiviteter hanteras? Hur ska vi ta in samtycke?

Vid en anmälan till exempelvis ett seminarium ger man sitt samtycke till att uppgiften lagras tillfälligt samt att personuppgifter också skickas till lokalen där seminariet hålls såsom preferenser i fråga om mat. Efter att seminariet är avklarat raderas uppgifterna.

Är det möjligt att använda en anmälningslista inför exempelvis ett seminarium för att veta vilka som anmält sig och vilka som behöver påminnas?

Ja, det är möjligt för att du ska kunna genomföra seminariet. När detta är avslutat raderar du listan.

Är det tillåtet att skriva om andra eller lägga ut bilder från aktiviteter och liknande på hemsidan?

Personerna som är med på bilderna har rättigheter enligt GDPR. Informera därför besökarna på aktiviteten att bilderna kan komma att användas för att informera om verksamheten på webbplatsen och att de har möjlighet att invända mot detta. Informera också om vem de i så fall ska kontakta.

Ni måste inte samla in namn på alla som är med på bilderna endast för att kunna följa reglerna i förordningen, men om någon identifierar sig själv och vill utöva sina rättigheter gäller rättigheterna i förordningen.

För mer information se länk till Datainspektionen.

https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/publicera-bilder-filmer-och-ljud/.

Är det tillåtet att publicera namn, arbetsplats och telefonnummer på lokalt förtroendevalda, skyddsombud och ledamöter i föreningens styrelse på arbetsgivarens interna hemsida?

Som förtroendevald förutsätts det att du är nåbar för medlemmar som måste kunna veta vilka som är förtroendevalda och hur dessa ska kunna kontaktas. Information på arbetsplatsens intranät är en enkel kontaktyta för medlemmar som alla anställda kommer åt.

I verksamhetsberättelse finns bl.a. en lista över vilka som har ingått i styrelsen samt innehaft andra förtroendeuppdrag för föreningen. Är detta tillåtet enligt GDPR?

Ja, det är tillåtet. En verksamhetsberättelse är en sammanställning över föreningens organisation och verksamhet under den senaste verksamhetsperioden. Förtroendevalda är offentliga och måste kunna redovisas för föreningens medlemmar.

Centrala begrepp inom GDPR

Ansvarsskyldighet: Dataskyddsförordningen ställer stora krav på dokumentation och att kunna visa att lagen efterlevs.

Behandling: Allting som kan kopplas till personuppgifter, exempelvis lagring, insamling, ändring, användning eller observation är personuppgiftsbehandling.

Berättigat intresse: En av de sex möjliga grunderna för laglig behandling av personuppgifter. Berättigat intresse ska inte misstas för att vara en sorts ”carte blanche” som ger organisationer möjlighet att fortsätta som tidigare med sin behandling av personuppgifter. En så kallad intresseavvägning måste alltid göras om den här rättsliga grunden ska användas.

Dataskydd som standard: Det finns tekniska och organisatoriska krav på att organisationer säkerställer säker hantering av personuppgifter. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet.

Dataskyddsombud (DPO): Ny befattning med fler formella krav än personuppgiftslagens personuppgiftsombud, förkortas DPO efter engelskans Data Protection Officer. Många, men inte alla, verksamheter är skyldiga att utse dataskyddsombud och anmäla detta till Datainspektionen innan 25 maj.

Incident: Om personuppgifter exempelvis har kommit på villovägar eller förstörts ska detta anmälas till Datainspektionen inom 72 timmar från det att man fick kännedom om incidenten. Ett gott samarbete med Datainspektionen är viktigt inte minst för att reducera de potentiellt väldigt höga böter som kan utfärdas.

Information: GDPR ställer stora krav på information till den som är registrerad, bl.a. ska informationen vara lättbegriplig. GDPR definierar i många fall vilken information som måste lämnas i olika situationer.

Laglig grund: Dataskyddsförordningens artikel 6 listar olika lagliga grunder, varav en måste vara uppfylld för att personuppgiftsbehandling ska få göras.

Personuppgift: I princip vad som helst som direkt eller indirekt kan användas för att identifiera en fysisk person.

Personuppgiftsansvarig: Den juridiska person som ansvarar för personuppgifter.

Personuppgiftsbiträde: Underleverantör som den personuppgiftsansvarige använder för att hantera personuppgifter.

Personuppgiftsbiträdesavtal: Ett obligatoriskt avtal mellan den personuppgiftsansvarige och biträdet som reglerar vad personuppgiftsbiträdet ska, och får, göra med personuppgifterna som behandlas för den personuppgiftsansvariges räkning.

Pseudonymisering: En dataskyddsåtgärd som innebär att personuppgifter avidentifieras i den databas de normalt används, men att det finns en nyckel tillgänglig på annat håll. Åtgärden ska inte förväxlas med kryptering eller anonymisering.

Samtycke: En av de sex möjliga grunderna för laglig behandling av personuppgifter. Samtyckesbegreppet utökas i förhållande till samtyckesbegreppet i personuppgiftslagen. Den som idag har inhämtat samtycke i enlighet med personuppgiftslagen har inte nödvändigtvis längre ett giltigt inhämtat samtycke när GDPR börjar tillämpas.

Uppgiftsminimering: En central princip i GDPR som handlar om att man inte får samla in fler personuppgifter än vad som är nödvändigt för ändamålet, och inte lagra uppgifter längre än nödvändigt.

Ändamål: Behandling av personuppgifter får endast ske med definierat ändamål och detta får i princip inte ändras eller utökas i efterhand.

Överföring: GDPR reglerar hur överföring av personuppgifter får ske, i synnerhet om uppgifter lämnas ut till någon, exempelvis ett personuppgiftsbiträde i ett land utanför EU. Om Storbritannien inte lyckas förhandla fram ett avtal med EU gällande dataskydd kommer även de att räknas som tredje land efter Brexit.