Uppdaterad:
2024-09-16

Frågor och svar om GDPR

EU-förordningen *general data protection (GDPR)*, eller dataskyddsförordningen som den heter på svenska, påverkar i hög grad hur vi som organisation behandlar och hanterar personuppgifter. Det kan emellertid vara svårt att hitta korrekt och handgriplig information om hur lagen ska omsättas i praktiken. Syftet med denna guide är därför att göra lagen mer lättillgänglig genom verksamhetsnära exempel. I denna guide hittar ni även rutiner för kontakten med Integritetsmyndigheten vid exempelvis personuppgiftsincidenter.

Grundläggande om GDPR:

Vad är GDPR?

25 maj 2018 ersattes Personuppgiftslagen (PUL) med EU-förordningen general data protection regulation (EU) 2016/679 eller dataskyddsförordningen som den heter på svenska. Lagen har till syfte att stärka skyddet för den personliga integriteten i samband med behandling av personuppgifter. Vi kommer hädanefter benämna lagen ”GDPR”.

Vilka är de grundläggande principerna enligt GDPR?

De grundläggande principerna är kärnan i dataskyddsförordningen och gäller för all personuppgiftsbehandling. Principerna innebär bland annat att anställda och förtroendevalda i PRO

- måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter
- bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål
- inte ska behandla fler personuppgifter än vad som behövs för ändamålen
- ska se till att personuppgifterna är riktiga
- ska radera personuppgifterna när de inte längre behövs
- ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs
- ska kunna visa att ni lever upp till dataskyddsförordningen och hur ni gör det.

Vad är en personuppgift?

Med personuppgift menas all information som direkt eller indirekt kan knytas till en fysisk, levande person. Även information som kan kopplas till en fysisk person med hjälp av kompletterande uppgifter trots kryptering eller pseudonymisering är personuppgifter.

Några exempel på personuppgifter:

- Namn

- E-post som förnamn.efternamn@företag.se
- Adress
- Telefonnummer
- Personnummer
- Medlemsnummer
- Foton
- Ljud- och filminspelningar

Vad är inte en personuppgift?

Avgörande för att något ska vara en personuppgift är att uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person. Exempel från Integritetsmyndigheten:

"Om en privatperson äger en bil är bilens registreringsnummer en personuppgift. Det är möjligt att utläsa att personen är bilägaren eftersom registreringsnumret kan kopplas till en fysisk person. Om bilen istället ägs av ett företag är registreringsnumret inte en personuppgift, eftersom bilen inte kan kopplas till en fysisk person."

Vad är en personuppgiftsbehandling?

Personuppgiftsbehandling är allting man gör när man behandlar personuppgifter såsom att samla in, spara, dela, sortera, publicera, lagra, förmedla, radera och så vidare.

Vad innebär det att personuppgifter ska gallras när de inte längre behövs?

En av grundprinciperna enligt GDPR är att man ska gallra personuppgifter när de inte längre behövs. Exempel på när du inte längre behöver en personuppgift är när du vidarebefordrat ett medlemsärende via e-post och fått återkoppling eller registrerat en medlem i medlemssystemet.

Vissa personuppgifter ska sparas enligt svensk lag (exempelvis bokföringslagen och lagen om anställningsskydd). Uppgifter som inte behövs för ändamålet ska dock alltid gallras. Om du exempelvis behöver spara deltagarlistor enligt bokföringslagen ska allt förutom namn gallras.

Vad räknas som en känslig personuppgift?

Vissa personuppgifter klassas som särskilt känsliga och de har därför ett starkare skydd. Följande uppgifter är så kallade känsliga personuppgifter:

- Etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i en fackförening
- Hälsa
- En persons sexualliv eller sexuella läggning
- Genetiska uppgifter
- Biometriska uppgifter som används för att entydigt identifiera en person

Vem granskar och verkställer tillämpningen av dataskyddsreglerna i Sverige?

Integritetsmyndigheten (IMY). Läs mer på deras hemsida www.imy.se.

Kan Integritetsmyndigheten komma att granska vår förening eller distrikt?

Integritetsmyndigheten kan välja att inrikta tillsyn mot vissa områden och branscher, så även vår. De kan även genomföra tillsyn av PRO vid en personuppgiftsincident eller klagomål på vår behandling av personuppgifter.

Vad sker vid en tillsyn?

Integritetsmyndigheten genomför normalt tillsyn på plats hos en organisation (inspektion) eller genom frågeformulär (skrivbordstillsyn). Om en inspektion ska genomföras får organisationen normalt information om detta i förväg. Om en organisation bryter mot GDPR har myndigheten följande befogenheter:

- Varningar
- Reprimander
- Förelägganden, inklusive begränsning och förbud
- Administrativa sanktionsavgifter

Rutin för klagomål, personuppgiftsincidenter och åberopande av rätten att bli bortglömd:

Vad är ett klagomål?

Vem som helst som anser att ni behandlar personuppgifter på ett felaktigt sätt kan lämna klagomål till Integritetsmyndigheten via deras e-tjänst. Även den som inte personligen berörs av behandlingen har möjlighet att lämna klagomål i form av "tips".

För att ett ärende ska betraktas som ett klagomål krävs följande:

- Klagomålet rör en brist vid behandling av personuppgifter som omfattas av dataskyddsförordningen (GDPR) eller brottsdatalagen (BDL).
- Personen som klagar själv berörs av behandlingen
- Den som behandlat uppgifterna kan identifieras
- Den som klagar är identifierbar och kontaktbar vid eventuella frågor.

Hur ska vi agera vid ett klagomål på vår personuppgiftsbehandling?

Om ni får meddelande från Integritetsmyndigheten om att en registrerad lämnat in klagomål på er behandling av personuppgifter ska ni skyndsamt skicka vidare ärendet till PRO Riks e-postadress info@pro.se. Ring för säkerhets skull även medlemsservice under PRO Riks öppettider.

Ärendet ska innehålla följande:

- Ämnesrad: "Klagomål från Integritetsmyndigheten".
- Innehåll: ditt namn, uppdrag och kontaktuppgifter samt meddelandet från Integritetsmyndigheten.

Uppdaterad:
2024-09-16

Vad är en personuppgiftsincident?

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter, obehörigt röjande av eller obehörig åtkomst till personuppgifter. En personuppgiftsincident kan medföra risker för den registrerades rättigheter eller friheter.

Incidenten kan leda till fysisk, materiell eller immateriell skada till exempel genom

- diskriminering, identitetsstöld, identitetsbedrägeri
- skadat anseende
- finansiell förlust
- brott mot sekretess eller tystnadsplikt.

Exempel på personuppgiftsincidenter enligt Integritetsmyndigheten (IMY):

- En obehörig part får tillgång till personuppgifter, till exempel om någon skickar personuppgifter till en mottagare som inte ska ha dem.
- Datorer som innehåller personuppgifter förloras eller stjäls.
- Någon ändrar personuppgifter utan tillstånd.
- Personuppgifter är inte längre tillgängliga för den som behöver dem och det leder till negativa konsekvenser för de registrerade.

Hur anmäler vi en personuppgiftsincident?

Anmäl skyndsamt personuppgiftsincidenten till PRO Riks e-postadress info@pro.se. Om PRO Riks gör bedömningen att incidenten behöver rapporteras till Integritetsmyndigheten (IMY) ska detta ske inom 72 timmar. Det är därför av yttersta vikt att ärendet tillskrivs högsta prioritet och att den som rapporterar in ärendet är tillgänglig. Ring för säkerhets skull även medlemsservice under PRO Riks öppettider.

Anmälan om personuppgiftsincident till PRO Riks kansli ska innehålla följande:

- Ämnesrad: “Personuppgiftsincident”.
- Innehåll: ditt namn, uppdrag och kontaktuppgifter samt beskrivning av incidenten.

Vad innebär rätten att bli bortglömd?

Rätten att få uppgifter raderade, eller rätten att bli bortglömd som det också kallas, innebär att alla som finns registrerade i våra system har rätt att vända sig till PRO och be om att få sina uppgifter raderade. När vi får in en begäran ska vi återkomma till den som åberopar sin rätt att bli bortglömd utan onödigt dröjsmål och senast inom en månad efter att ha vi har fått in begäran. Huruvida man faktiskt har rätt att bli bortglömd är beroende av flera faktorer. Exempelvis kan inte en person som har ett aktivt medlemskap i PRO begära att bli bortglömd.

Hur hanterar vi åberopande av rätten att bli bortglömd?

Uppdaterad:
2024-09-16

Om en registrerad åberopar rätten att bli glömd eller efterfrågar dokumentation över de personuppgifter ni behandlar i PRO:s gemensamma system ska ni skicka vidare ärendet till PRO Riks e-postadress info@pro.se.

Ärendet ska innehålla följande:

- Ämnesrad: ”Rätten att bli bortglömd” alternativt ”Personuppgiftsutlämning”
- Innehåll: ditt namn, uppdrag och kontaktuppgifter och den registrerades medlemsnummer alternativt personnummer

Exempel från verksamheten:

Vems personuppgifter behandlar PRO?

PRO behandlar följande kategoriers personuppgifter:

- Medlemmar
- Förtroendevalda
- Medlemmars ställföreträdare (gode män, förmyndare och anhöriga)
- Allmänheten (t.ex. frågor som inkommer via e-post)
- Externa samarbetspartners
- Anställda

Var behandlar PRO personuppgifter?

Olika delar av organisationen behandlar personuppgifter på olika platser. Föreningar behandlar exempelvis personuppgifter i medlemssystemet ”Harald”, E-postklienten ”Outlook” och webbsideverktyget ”Sitevision”. Rikskansliet, som ansvarar för avisering och ekonomi, behandlar även personuppgifter i aviseringsprogram och olika fildelningstjänster.

Är alla bilder och filmer där personer förekommer personuppgifter?

Utgångpunkten är att alla bilder och filmer där personer förekommer är personuppgifter. Det går nämligen inte att på förhand avgöra vad som är en identifikationsmarkör. Bara för att någon till exempel fotograferas bakifrån betyder det inte att personen är oidentifierbar. Personen kan ha en tatuering, frisyr, hållning eller liknande som vissa lätt känner igen.

Vad är viktigt att tänka på vid publicering av bilder på personer i digitala kanaler?

Vi arbetar på att ta fram riktlinjer för fotografering och filmupptagning för organisationen. Tillsvidare ska ni alltid följa de grundläggande kraven för publicering av bilder i digitala kanaler. Här nedan har vi sammanfattat kraven utifrån premissen att ni fotograferar eller filmar under ett möte eller aktivitet.

Före aktiviteten
Om ni arrangerar en aktivitet eller bjuder in till möte där ni skickar ut inbjudan ska det framgå att ni kan komma att fotografera eller filma samt i vilka kanaler bild och film kan komma att publiceras. Ni ska också informera om vem man kan vända sig till om man inte vill vara med på bild eller film.
Under aktiviteten

Informera muntligt att ni kan komma att fotografera eller filma samt vem man ska vända sig till om man inte vill vara med på film eller bild. Sätt även upp affischer där ni informerar om att ni kan komma att fotografera eller filma samt i vilka kanaler dessa filmer och bilder kan komma att publiceras. Att informera via affischer är framförallt en fördel om ni anordnar öppna aktiviteter som inte kräver föranmälan eller aktiviteter där ni inte kan informera alla på en och samma gång.

Obs! Bestäm er för hur ni rent praktiskt ska gå tillväga om personer inte vill vara med på bild eller film. Kanske kan de få ett diskret klistermärke eller annan markör som gör att det blir enkelt för den som fotograferar eller filmar att anpassa sig istället för att personer som inte vill vara med på bild eller film måste avlägsna sig från olika sammanhang.

Kan vi exportera medlemsuppgifter från medlemssystemet till annan plats?

Ja och nej. Ni kan exportera medlemsuppgifter och skriva ut medlemslistor för specifika ändamål – som att pricka av deltagare under möten, dela ut post och så vidare. Kom ihåg att inte skriva ut eller exportera fler uppgifter än vad ni behöver för ändamålet samt att makulera listan när den inte längre behövs. Fråga emellertid er varför ni behöver skriva ut listan. Kan ni utföra uppgiften utan att skriva ut eller exportera till annan plats? Är det möjligtvis bristande kunskap om hur ni använder rapporterna i medlemssystemet som ligger till grund för att ni exporterar eller skriver ut?

Kan vi lagra medlemslistor på annan plats än medlemssystemet?

Ja och nej. Att exportera personuppgifter från medlemssystemet för lagring på annan plats är enbart tillåtet om ni behöver spara uppgifterna enligt svensk lag (såsom bokföringslagen). Det är till exempel inte motiverat eller ändamålsenligt enligt GDPR att exportera medlemsuppgifter i form av en extern medlemslista i Excel eller pärm för att det underlättar hanteringen eller kan vara "bra att ha".

Kan vi lägga till medlemmars telefonnummer i medlemssystemet genom att söka på sidor som "Eniro.se", "Hitta.se" och "Ratsit.se"?

Nej. Det är olämpligt ur GDPR-synpunkt. Enligt GDPR har ni skyldighet att säkerställa att personuppgifterna är riktiga och uppdaterade och dessa kostnadsfria tjänster har inte samma krav på korrekthet som de betaltjänster som finns på marknaden som uppdateras mot Statens personregister (SPAR). Det är dessutom väldigt vanligt att målgruppens mobilabonnemang är skrivna på en annan person.
Detta förfarande kräver även att ni gör en riskanalys, skapar en rutin för hur ni säkerställer att ni registrerar rätt uppgifter samt informerar de registrerade. Det är helt enkelt väldigt mycket jobb för något som enkelt kan lösas på annat sätt. Ett bättre förfarande är att ni istället är noga med att samla in alla uppgifter från första början eller samlar in eventuella uppgifter när ni träffar medlemmen i fråga.

Kan vi ge ut förtroendevaldas kontaktuppgifter som inte finns på PRO:s nya hemsida?

Nej, står inte kontaktuppgifterna som personen söker på distriktets, samorganisationens eller föreningens hemsida ska ni inte ge ut dessa kontaktuppgifter. Den gamla hemsidan speglade kontaktuppgifter till styrelsen från medlemsystemet men på den nya hemsidan måste man manuellt skriva in de kontaktuppgifter man vill ska vara synliga. På så vis säkerställer vi att enbart de som vill

ha sina uppgifter synliga kontaktas. Den här förändringen ger även distrikt, förening och samorganisation möjlighet att själva styra över inflödet av ärenden samt att vi reglerar användningen av privat e-post.

Kan vi göra massutskick via SMS till medlemmar från en privat mobil?

Nej, det är mycket olämpligt ur GDPR-synpunkt. Använd istället verktyget som finns i medlemssystemet för utskick av e-post och sms.

Kan vi lägga in medlemmars e-post efter att de har mejlat oss?

Ja, om de är medlemmar har ni laglig rätt att lägga in deras e-post i medlemssystemet.

Kan vi lagra personuppgifter i e-postklienten Outlook?

Nej. E-post är inte en säker förvaring och det kan vara svårt att hitta uppgifter om en enskild eller säkerställa att uppgifterna blir borttagna när de inte längre behövs. Ha därför för vana att gallra e-post så fort ni har vidarebefordrat ärenden eller överfört medlemsuppgifterna till medlemssystemet. Integritetsmyndigheten är mycket tydlig med att man ska undvika att använda e-post som lagringsplats så långt det är möjligt eftersom det är en kanal som ständigt utsätts för bedrägeriförsök (så kallad phising) samt att överföringen av data inte är skyddad.

Kan vi hantera medlemsärenden i privat e-post

Nej, detta är något vi håller på att fasa ut eftersom det är olämpligt ur GDPR-perspektiv. På distriktsnivå kan man använda sin personliga PRO-adress men på föreningsnivå ska man enbart använda föreningens info-adress i kommunikationen med medlemmar. Användandet av privat e-post är en av de absolut största riskerna för PRO som organisation, speciellt med tanke på den stora ökningen av bedrägerier mot gruppen äldre.

Kan vi göra massutskick via e-post till våra medlemmar?

Ja, men använd verktyget som finns i medlemssystemet för utskick av e-post och sms. Rapporten tar hänsyn till de som inte vill bli kontaktade samt att ni minimerar risken att utskicket flaggas som skräppost av mottagarnas e-postklient. Om ni av någon anledning måste använda Outlook till att skicka e-post till utvalda medlemmar ska ni alltid använda funktionen “hemlig kopia”. På så sätt blir mottagarlistan dold för mottagarna.

Kan jag som förtroendevald skicka medlemslistor via e-post till en annan förtroendevald med uppdrag?

Nej, det är mycket olämpligt ur GDPR-synpunkt. E-post är inte en säker kanal. Det innebär även att man kringgår behörighetssystemet som finns inbyggd i medlemssystemet. Lösningen är därför att ge förtroendevalda behörighet till medlemslistan i medlemssystemet i stället.

Får vi behandla känsliga uppgifter via e-post?

Ja och nej. PRO har ingen laglig rätt att behandla känsliga personuppgifter men vi kan inte styra över innehållet i ärenden som skickas in via e-post. Grundregeln är därför att e-post med känsliga personuppgifter ska raderas direkt när ärendet hanterats. Det är exempelvis vanligt att medlemmar

uppger sjukdomshistorik som förklaring till varför de väljer att avsluta sitt medlemskap. Se därför till att informera era medlemmar om att inte ange känsliga personuppgifter i kommunikationen med er förening, samorganisation eller distrikt. Ni kan förslagsvis informera om detta i ert automatiska e-postsvar och på er kontaktsida.

Kan vi spara bifogade filer i vår e-post?

Ja och nej. Det är tillåtet att lagra bifogade filer i e-posten som inte innehåller personuppgifter. Det kan dock bli svårt att upprätthålla gallringsreglerna som GDPR uppmanar till om man använder e-post som lagringsplats. Rekommendationen är därför att ladda upp bifogade filer som ni vill spara i molntjänsten "Onedrive"" som ingår i Microsoft 365".

Vidare läsning

Integritetsmyndighetens hemsida

www.integritetsmyndigheten.se

LAS (Lagen om anställningsskydd)

https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/lag-198280-om-anstallningsskydd_sfs-1982-80/

Bokföringslagen

https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/bokforingslag-19991078_sfs-1999-1078/

EU:s riktlinjer för personuppgiftsincidenter

https://edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_sv.pdf