Lathund GDPR

Vad är GDPR

- GDPR står för General Data Protection Regulation och heter på svenska Dataskydds-förordningen.
- Lagen handlar om hur organisationer, företag och myndigheter får behandla personuppgifter. Det gäller både digital och analog/manuell (exempelvis listor/register som förs på papper) behandling. Den här lagen kommer att ersätta den lag vi idag har, som heter Personuppgifts-lagen, brukar förkortas PUL.
- Det övergripande syftet med GDPR är att stärka individens rätt till sina personuppgifter och där-igenom stärka den personliga integriteten.
- GDPR träder i kraft i maj 2018 och gäller alla medlemmar i EU. Det innebär att alla organisationer, företag och myndigheter behöver göra en del förändringar när det gäller hur person-uppgifter behandlas. Det gäller såklart även för Svenska Röda Korset.

Vad är en personuppgift?

- **Personuppgift**: En personuppgift är alla typer av uppgifter som gör att man kan identifiera en fysisk levande person. Det kan till exempel vara namn, personnummer, adress, telefonnummer, e-post, foton och kontouppgifter. Det kan också vara uppgifter som inte för sig själva gör att man kan identifiera en person, exempelvis kön och ålder. Utifrån bara kön och ålder kan du inte identifiera en specifik person, men om du däremot kan koppla de uppgifter till andra uppgifter du har, så kan de uppgifterna tillsammans identifiera specifika personer. Då utgör alltså dessa uppgifter tillsammans en personuppgift.

  Exempel: kretsen registrerar en ny medlem och ber om namn, personnummer, adress, telefonnummer och e-postadress. Samtliga dessa är personuppgifter. Men om kretsen bara skulle be om personens e-post och denna är svampen@hotmail.com, så kan enbart denna inte identifiera en person och är i sig själv inte en personuppgift. Men så fort något annat, exempelvisnamn och adress, kan knytas till e-postadressen kan den utgöra en personuppgift. Att bara registrera "kvinna 45 år" är inte personuppgift. Det är också så man kan avidentifiera en person, exempelvisgenom att bara spara uppgifter om kön och ålder.

- **Känsliga personuppgifter**: Vissa uppgifter om individer klassas dock som särskilt skyddsvärda eller känsliga personuppgifter, exempelvis etnicitet, sexuell läggning, religiös inriktning och politiskt åskådning. Sådana uppgifter ska vi inte samla in. Vissa undantag kan finnas vid exempelvis vid Svenska Röda Korsets verksamhet med efterforskning och familjeåterförening samt vid viss patientklassad verksamhet.

- **Behandling av personuppgifter:** När vi säger behandling av personuppgifter, menar vi exempelvis lagring, läsning och bearbetning. Det kan handla om att upprätta listor över personer, registrera personer som till exempel frivilliga eller medlemmar och att använda uppgifterna till att kontakta personer eller till att skicka ut information –det vill säga allt vi gör med personuppgifter.

På vilken grund får kretsen behandla personuppgifter?

All personuppgiftsbehandling måste kunna motiveras med hänvisning till någon av de olika lagliga grunderna som finns i GDPR. En laglig grund som ofta nämns i GDPR-sammanhang är den som kallas **samtycke**. Vi har tillsammans med FRII och i konsultation med jurister, kommit fram till att vi inte kommer att stödja oss mot samtycke som laglig grund, utom i specifika fall, exempelvis inom Efterforskning och familjeåterförening.

De lagliga grunder som i stället blir aktuella är:

- **Fullgörande av avtal**: den här lagliga grunden kan vi stödja oss emot när det gäller den personuppgiftsbehandling som sker när någon blir och är medlem, frivillig eller månadsgivare.
- **Rättslig förpliktelse:** för att kunna använda sig av rättslig förpliktelse som laglig grund krävs det att personuppgiftsbehandlingen är nödvändig på grund av en annan lag, exempelvis enligt bokföringslagen. Den här grunden blir alltså aktuell för de kretsar som exempelvis administrerar löner, fakturor eller patientinformation som regleras i lag.
- **Berättigat intresse:** den här lagliga grunden kan vi stödja oss emot för exempelvis behandling i informationssyfte, marknadsföringssyfte, analyssyfte eller undersökningssyfte. Det här förutsätter dock att vi tydligt har informerat den enskilde individen om vad vi avser att göra med personuppgifterna och att Svenska Röda Korset med hänsyn till vår verksamhet anses ha ett berättigat intresse. Det handlar alltså inte om att samla in ett aktivt samtycke, utan om att informera tydligt om hur vi behandlar personuppgifter om individen väljer att bli medlem, frivillig eller givare. Du kan läsa mer nedan om hur en sådan informationstext kan utformas.

På vilket sätt tar GDPR hänsyn tillindividens rättigheter?

Den nya lagen sätter individens integritet i centrum och utgår ifrån ett antal grundläggande rättigheter, exempelvis:

- **rätt till information:** som enskild individ har du rätt att få information om när och hur dina personuppgifter behandlas och vad de används till, dels när uppgifterna samlas in, dels när du själv begär det.
- **rätt till rättelse:** som enskild individ har du rätt till att få felaktiga uppgifter om dig rättade eller kompletterade.
- **rätt till radering (kallas även ”rätten att bli bortglömd”)**: som enskild individ har du rätt att få dina uppgifter raderade. Det gäller inte i de fall där det finns lagkrav på att behandlingen måste finnas kvar, exempelvis enligt Patientlagstiftningen eller bokföringslagen.
- **rätt till begränsning:** som enskild individ har du rätt att få dina uppgifter begränsade. Det betyder att du kan begära att dina uppgifter markeras och enbart används för vissa avgränsade syften, exempelvis att du som individ inte önskar bli kontaktad per telefon eller e-post.

Hur ser ansvarsfördelningen mellan kretsar och tjänstemannaorganisation ut?

GDPR ställer ett krav på att någon part måste vara ansvarig för den behandling av personuppgifter som sker. Eftersom Svenska Röda Korsets organisation är uppdelad i en tjänstemannaorganisation och kretsar, där personuppgifter behandlas av båda parter, så behöver vi fastställa vem som bär ansvar för behandlingen av personuppgifter.

Vi har tidigare i Kretsnytt kommunicerat att tjänstemannaorganisationen och kretsarna behöver ingå ett avtal gällande ansvarsfördelningen för personuppgifter. Efter att ha undersökt frågan ytterligare tillsammans med jurister har vi dock kommit fram till att ett sådant avtal inte behövs. I stället kan vi konstatera att tjänstemannaorganisationen och kretsarna har ett gemensamt ansvar för behandling av personuppgifter. Det innebär:

- att kretsen och tjänstemannaorganisationen gemensamt ansvarar för den personuppgiftsbehandling som sker i de system som både krets och tjänstemannaorganisation använder, alltså Redy och Frivillig,
- inte att kretsarna bär ansvar för den behandling som bara sker inom tjänstemannaorganisationen,
- inte att tjänstemannaorganisationen bär ansvar för den behandling som bara sker i kretsarna, exempelvis deltagarlistor och boendeplatslistor, som ju inte behandlas i de system och plattformar som tjänstemannaorganisationen tillhandahåller.

Exempel: i REDY kan både Infoservice och kretsar registrera en medlem och även ändra uppgifter eller avsluta ett medlemskap. Kretsarna och tjänstemannaorganisationen har alltså ett gemensamt ansvar förpersonuppgifterna i REDY. Men det betyder inte att alla kan göra allt med uppgifterna. Kretsarna kan exempelvis inte behandla personuppgifter i samband med gåvor till Svenska Röda Korset centralt.

I Frivillig har i stället kretsarna större behörighet än tjänstemannaorganisationen. Det finns system som inte kretsarna har tillgång till och för dessa ansvarar endast tjänstemannaorganisationen. På samma sätt har inte tjänstemannaorganisationen personuppgiftsansvar för de personuppgifter som kretsar behandlar i exempelvis egna Excel-filer eller med manuella listor.

Vad behöver kretsen vidta för åtgärder?

Nu vet vi vad en personuppgift är, vad som menas med behandling av personuppgifter och hur ansvars-fördelningen ser ut. Nu undrar ni säkert vad det här innebär för er mer konkret?

- **Utse dataskyddsansvarig:** Enligt GDPR finns det i vissa fall ett obligatoriskt krav på att en personuppgiftsansvarig behöver utse ett så kallat Dataskyddsombud. Med hänsyn till exempelvis omfattning av personuppgiftsbehandling så finns det dock inget sådant krav för Svenska Röda Korsets kretsar. I de fall något sådant krav inte finns, rekommenderar GDPR att det är ändå är lämpligt att utse någon som är dataskyddsansvarig. Den personen kan exempelvis vara samordnare för vilka åtgärder som kretsen behöver genomföra för att uppfylla GDPR och att rutiner följs.
- **Gör en kartläggning**: Till att börja med behöver ni gå igenom på vilka olika sätt ni behandlar personuppgifter –det innebär att ni behöver kartlägga vilka register eller listor ni har, både digitala och analoga/manuella och vilka personuppgifter ni behandlar i dem. Ni behöver också tydliggöra vilka har som har möjlighet att se, ändra eller ta bort uppgifter samt vem eller vilka i kretsen som har ansvar och behörighet

att genomföra rättelser, raderingar eller övriga administrativa uppgifter som gäller er personuppgiftsbehandling.

En kartläggning kommer såklart för många av er tydliggöra att ni har en viss behandling av personuppgifter utanför de system eller plattformar som tjänstemannaorganisationen tillhandahåller. Som en del i kartläggningen behöver ni därför göra en bedömning om det är nödvändigt med en sådan behandling, eftersom det medför ett utökat ansvar för kretsen.

För att göra en kartläggning kan ni använda er av exempelvis ordbehandlingsprogrammet Word eller liknande, eller Excel. Skriv upp vilka register ni har, både manuella och digitala. Gå igenom och dokumentera vart och ett av dem utifrån frågeställningarna nedan. Listan är inte avsedd att vara uttömmande, men ett mycket bra hjälpmedel för att komma igång med er kartläggning.

- Behandlas personuppgifter? Om ja, gå vidare.
- Vilka personuppgifter behandlas (namn, personnummer etcetera)?
- Har ni en möjlighet att sammanställa personuppgifter för en viss person? Vad gör ni om en person hör av sig och vill veta vilka personuppgifter ni har på hen?
- Vilka kategorier av personer behandlas (givare, medlemmar, frivilliga etcetera)?
- Sker en automatisk eller manuell inmatning av personuppgifterna?
- Behandlas känsliga personuppgifter (till exempel etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv)?
- Behandlas skyddade personuppgifter?
- Inhämtas samtycke i samband med att ni efterfrågar personuppgifter?
- Informeras personen om hur ni kommer att använda personuppgifterna?
- Görs en ålderskontroll?
- Vilka rutiner finns för att gallra och ta bort personuppgifter?
- Lämnas personuppgifterna till någon annan externt?
- Lämnas personuppgifterna till någon annan internt?

- **Minimering av uppgifter:** En viktigprincip inom GDPR är att försöka minimera behandlingen av personuppgifter. För Svenska Röda Korset innebär det att göra medvetna val gällande de personuppgifter som samlas in och att kunna motivera den behandling som sker. Vi behöver därför vara restriktiva med vilka uppgifter vi samlar in och varför. Det handlar exempelvis om att inte skapa externa listor eller register i de fall där det inte absolut är nödvändigt eller att samla in mer information om personer än vad som kan motiveras med hänvisning till verksamhetens ändamål. Det kanske inte alltid är nödvändigt med personnummer, ibland räcker det kanske bara med namn och telefonnummer.

  Exempel: att minimera behandlingen av personuppgifter kan handla om att inte använda personuppgifter i e-post-kommunikation. Om ett utskick ska göras ska inte mottagarna kunna se vilka övriga som får utskicket, då vi i så fall har spridit personuppgifter. Hur du går till väga för att skicka ett mail till en sändlista utan spridning av personuppgifter, klicka här (https://support.microsoft.com/sv-se/office/d%C3%B6lja-namn-och-adresser-i-en-personlig-distributionslista-a49b5738-5da1-4f54-9f8b-f1033edce299?ui=sv-se&rs=sv-se&ad=se).

- **Informera om vår behandling**: Tänk på att vi alltid måste informera om hur vi behandlar personuppgifter när vi samlar in dem. Det kan göras genom att exempelvis hänvisa till Svenska Röda Korsetsdataskyddspolicy som kommer att finnas på redcross.se från och med maj 2018 och genom att hänvisa till de rutiner och processer kretsen har för sin behandling.

- **Skydd mot obehörig behandling**: Tänk på att obehöriga personer inte ska få tillgång till personuppgifter. Lämna därför inte datorer, surfplattor, telefoner, papper, pärmar eller annat material som innehåller personuppgifter på ett sådant sätt så att obehöriga kan få tillgång till dessa. Se också till att ni har rutiner för lösenord och behörigheter för de system ni använder er av.

- **Lagring av personuppgifter**: se till att inte spara personuppgifter längre än vad som är nödvändigt. Vi kan exempelvis spara en individs personuppgifter så länge individen är fortsatt frivillig, medlem eller månadsgivare. Personuppgifter för individer som har varit inaktiva i mer än tre år måste vi ta bort eller anonymisera. Lika viktigt som det är att ha rutiner för hur ni samlar in personuppgifter, lika viktigt är det att ha rutiner för hur och när ni tar bort personuppgifter.

- Kretsen behöver känna till **den enskilda individens rättigheter** som vi har nämnt tidigare. Om kretsen själva inte kan administrera exempelvis en individs önskan om att rätta, lägga till eller ta bort sina uppgifter, ska kretsen ge personen kontaktuppgifter till Svenska Röda Korsets Infoservice.

- Även om kretsen enbart använder centrala system och plattformar, behöver kretsen ändå göra den kartläggning som beskrevs tidigare.

- Kretsen behöver ta del av och känna till Svenska Röda Korsets Dataskyddspolicy och var den finns.

Hur lever kretsen upp till informationsskyldigheten?

Informationsskyldigheten innebär mer konkret att när ni inhämtar personuppgifter, exempelvis när ni värvar medlemmar eller frivilliga, är skyldiga att informera om hur ni kommer att behandla deras personuppgifter. Om kretsen endast behandlar i de system som tjänstemannaorganisationen tillhandahåller, räcker det med att hänvisa till Svenska Röda Korsets Dataskyddspolicy.

I de fall där kretsen även har en personuppgiftsbehandling utöver tjänstemannaorganisationens system, behöver kretsen utforma en egen informationstext där det framgår hur ni behandlar personuppgifter i olika situationer.

Förutom att få en översikt över vilka register eller listor ni har, både digitala och analoga/manuella, syftar den kartläggning vi tidigare beskrivit till att tydliggöra för er själva, och för eventuell oberoende granskare, att ni har kontroll över er personuppgiftsbehandling samt att ni har sett över er behandling med hänsyn till de krav GDPR ställer.

Denna informationstext ska inte enbart vara ett internt dokument. I kontakt med medlemmar eller frivilliga ska kretsen även hänvisa till informationstexten.

Som tidigare påpekats har Svenska Röda Korset och kretsarna ett gemensamt personuppgiftsansvar för behandling i de system som tillhandahålls av tjänstemannaorganisationen. Därför

behöver kretsen i sin informationstext också hänvisa till Svenska Röda Korsets Dataskyddspolicy när det gäller sådan behandling.

För att komma igång med skrivandet av informationstexten kan kretsen ta hjälp av nedanstående frågor/rubrikförslag:

- Varför samlar vi in personuppgifter?
- Vi behandlar personuppgifter i huvudsak för att:
- Vilka personuppgifter samlar vi in och när?
- Vem får tillgång till dina personuppgifter?
- På vilken laglig grund behandlar vi dina personuppgifter?
- Dina rättigheter till tillgång, rättelse och radering
- Hur länge lagras dina personuppgifter?
- Hur kontaktar du oss?

Vilka rutiner behöver kretsen se över?

- När det gäller **individens rättigheter** som nämnts ovan, behöver kretsen säkerställa att samtliga dessa rättigheter uppfylls. Det betyder exempelvis att kretsen se över sina rutiner kring hur enskild individ kan få sina uppgifter rättade eller kompletterade samt hur en enskild individ efter förfrågan ska kunna få information om när och hur personuppgifterna behandlas.
- **Borttagning av personuppgifter**: efter tre års inaktivitet eller att individen önskar bli borttagen behöver kretsen se över sina rutiner för hur kretsen tar bort individens personuppgifter ur alla system och listor/register. Det kan ju dock vara så att kretsen skulle vilja ha kvar uppgifter för att kunna föra statistik, exempelvis hur många personer som deltagit i en kurs som kretsen haft. För att kunna föra sådan statistik finns möjlighet att anonymisera personuppgifterna. Det betyder att kretsen behöver radera de personuppgifter som gör det möjligt att identifiera en specifik individ, exempelvis namn, telefonnummer, e-postadress, postadress eller personnummer. För statistiska syften räcker det ofta att enbart spara exempelvis kön, ålder och kanske postort.