Lathund för GDPR

Det är viktigt att komma ihåg att eftersom Dataskyddsförordningen (GDPR) gäller i alla EU:s medlemsländer så är lagen också bred och innefattar många olika delar. Länderna inom EU har olika förutsättningar och olika utgångslägen, vilket innebär att lagen kan medföra olika anpassningar beroende på vilket land som åsyftas.

För svensk del innebär GDPR, kanske framförallt, att vi behöver se över vår syn på hur öppen personuppgiftsbehandlingen egentligen bör och får vara. Vi är ju i Sverige vana med att det är lätt att komma över personuppgifter genom några enkla sökningar online. Det kommer det nog att fortsatt vara, men kanske med en högre kännedom om hur behandlingen faktiskt ser ut för gemene person – alltså att vi får en ökad transparens kring hur våra personuppgifter behandlas. Detta är något som på sikt kan gynna oss på SRK eftersom vi värnar högt om individers integritet och deras förtroende för oss – också vad gäller hur vi behandlar deras personuppgifter.

Vad är GDPR?

- GDPR står för General Data Protection Regulation och heter på svenska Dataskyddsförordningen.
- 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 Personuppgiftslagen, brukar förkortas PUL.
- Det övergripande syftet med GDPR är att stärka individens rätt till sina personuppgifter och därigenom 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 personuppgifter behandlas. Det gäller såklart även för Svenska Röda Korset.

Vad är en 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: Svenska Röda Korset registrerar en ny medlem och ber om namn, personnummer, adress, telefonnummer och e-postadress. Samtliga dessa är personuppgifter. Men om Svenska Röda Korset 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, exempelvis namn och adress, kan knytas till e-postadressen kan den utgöra en personuppgift. Att bara registrera "kvinna 45 år" är inte personuppgift. Vi kan också avidentifiera en person, exempelvis genom 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, exempelvis vår verksamhet med efterforskning och familjeåterförening samt vid viss patientklassad verksamhet.

Vad innebär behandling av personuppgifter?

När vi säger behandling av personuppgifter, menar vi exempelvis följande:

- **Lagring:** Lagring innefattar all typ av sparande av personuppgifter. Det vanligaste exemplet på lagring är digitala system som har till uppgift att spara/lagra personuppgifter. För Svenska Röda Korset är CRM ett bra exempel, där det finns en mängd personuppgifter som sparas för olika syften. Det finns även andra system hos oss där personuppgifter sparas/lagras. Att lagra/spara personuppgifter i olika digitala system är alltså att anse som behandling av personuppgifter. Det spelar alltså ingen roll om personuppgifterna används aktivt, exempelvis för att kontakta personer, eller om personuppgifter enbart sparas i digitala register av andra skäl.

- **Manuella listor:** det är viktigt att komma ihåg att GDPR inte bara gäller digital behandling. Till skillnad från Personuppgiftslagen så omfattar GDPR även det som Personuppgiftslagen gjorde undantag för, så kallat ostrukturerat material. Det innebär att de personuppgifter du har i manuella listor, exempelvis i fysiska mappar och pärmar, men även i dokument på din dator, utanför de centrala systemen, är behandling av personuppgifter om omfattas därför av kraven i GDPR.

- **Segmentering:** Svenska Röda Korset behandlar en stor mängd personuppgifter och ibland utförs så kallade segmenteringar av data. Det innebär att personuppgifter struktureras efter vissa kriterier, exempelvis ålder och postort. Det kan alltså ibland vara intressant att exempelvis veta hur många personer mellan 20-30 års ålder boendes i Helsingborg som skänkte en gåva till en särskild insamlingskampanj. Segmentering är alltså ytterligare ett exempel på hur personuppgifter kan behandlas i Svenska Röda Korsets verksamhet.

- **Postala utskick:** vi behandlar personuppgifter när vi exempelvis skickar ut givarbrev till potentiella eller befintliga givare, när vi skickar ut Henry eller när vi skickar ut inbetalningskort till våra medlemmar.

- **Telemarketing:** vi använder personuppgifter för att kunna kontakta individer per telefon, både i marknadsföringssyfte men också exempelvis för att se om månadsgivare skulle kunna höja sin månatliga gåva. För att kunna höra av oss till olika individer behöver vi använda oss av personuppgifter, i detta exempel telefonnummer. Så fort vi kontaktar en individ har vi alltså behandlat personuppgifter.

De exempel som är angivna ovan är bara några olika typer av personuppgiftsbehandling. Det är viktigt att komma ihåg att så fort en uppgift som går att härleda till en fysisk levande person använts, här gäller alltså också även om uppgifterna endast sparats i ett register, så har vi behandlat personuppgifter. För Svenska Röda Korset innebär det att det mesta i vår verksamhet berör just personuppgiftsbehandling. Det innebär dock inte att det skulle vara

problematiskt eller felaktigt att göra så – men vi behöver givetvis vara noga med att vi följer de regler och riktlinjer som finns.

- **Dokumentation:** oavsett på vilket sätt vi behandlar personuppgifter så ställer GDPR krav på dokumentation. Det betyder att vi behöver dokumentera på vilka sätt vi samlar in och behandlar personuppgifter, både digitalt och manuellt. För viss sådan behandling finns idag redan dokumenterade rutiner, medan vi för andra behandlingar behöver se över befintliga rutiner och upprätta dokumentation, exempelvis vad gäller information, gallring och radering.

På vilken grund får Svenska Röda Korset 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 använda oss av samtycke som laglig grund, utom i specifika fall, exempelvis inom vår verksamhet med efterforskning och familjeåterförening.

De lagliga grunder som istället 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 eller månadsgivare. Detta på grund av att både medlemskapet och månadsgivandet i laglig mening anses utgöra en form av avtal.

- **Rättslig förpliktelse:** för att kunna använda oss av rättslig förpliktelse som laglig grund krävs det att personuppgiftsbehandlingen är nödvändig på grund av en annan lag, exempelvis enligt Bokföringslagen, Patientlagstiftning, Sekretesslagen och Tryckfrihetsförordningen. Dataskyddsförordningen (GDPR) är en subsidiär lag, vilket innebär att andra lagar som innehåller bestämmelser kring personuppgiftsbehandling är överordnad GDPR.

- **Berättigat intresse:** GDPR beskriver det berättigade intresset som en intresseavvägning som kan göras mellan oss som personuppgiftsansvarig och den enskilda individen. En intresseavvägning innebär att vår organisations verksamhet att inhämta och behandla personuppgifter överväger individens rätt att inte få sina personuppgifter behandlade.

  Berättigat intresse som laglig grund 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.

På vilket sätt tar GDPR hänsyn till individens 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. Här handlar det alltså om att vi som organisation alltid måste informera om vår behandling i alla de fall där vi samlar in personuppgifter. Oftast kommer detta att handla om att vi lägger till en kort informationstext där vi också länkar till vår Dataskyddspolicy.

- **Rätt till rättelse:** som enskild individ har du rätt till att få felaktiga uppgifter om dig rättade eller kompletterade. Den här rättigheten kommer nog vanligast att åberopas genom att individen hör av sig till oss på grund av ändringar i personens adress, telefonnummer eller liknande.

- **Rätt till radering (kallas även ”rätten att bli bortglömd”):** som enskild individ har du rätt att få dina uppgifter raderade. Här handlar det alltså bland annat om att en individ har rätt att invända emot vår behandling, och oavsett individens skäl är vi då skyldiga att radera individens personuppgifter (här har vi möjlighet att avidentifiera, vilket vi också kommer att använda oss av i många fall). Denna rättighet kan åberopas i de fall där det inte finns lagkrav på att behandlingen måste finnas kvar, exempelvis enligt patientlagstiftning 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. Detta sker redan i viss utsträckning och innebär inga egentliga skillnader från hur det redan fungerar. Även vi som organisation har ju ett intresse av att inte kontakta personer på ett sätt de inte önskar.

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.

Tjänstemannaorganisationen och kretsarna har dels ett ***gemensamt***, dels ett **eget** 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 för personuppgifterna 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 istället 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 du tänka på?

- **Minimering av uppgifter:** En viktig princip 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.

  Mejl:

  GDPR gör gällande att personuppgifter inte bör delas via e-postkommunikation.

  Eftersom e-postkommunikation ofta är det vanligaste sättet att kommunicera både internt och extern i dag, är just denna regel lite problematisk. GDPR berättar heller inte hur alla organisationer eller företag ska lösa detta rent tekniskt, eller vilka andra typ av lösningar som kan användas. Av den anledningen behöver vi, och alla andra organisationer och företag, komma fram till en rimlig lösning på detta fram till dess att vi får ytterligare klargöranden från Datainspektionen. En del av en lösning på sikt skulle kunna vara krypterad e-postkommunikation, vilket också är något Svenska Röda Korset ser över.

  Utgångspunkten är alltså att vi inte ska skicka personuppgifter via mejl. Det finns dock situationer i vår verksamhet där det inte finns någon annan teknisk eller manuell lösning. Ett exempel är viss internationell verksamhet, där det idag inte finns andra lämpliga gemensamma plattformar för att dela personuppgifter. I detta och andra undantagsfall och där exempelvis PUFF eller G inte är tillräckliga, är det viktigt att du dokumenterar vilka rutiner du har för hur du behandlar personuppgifter via mejl. Det behöver göras för att vi ska kunna säkerställa hur vi exempelvis rensar mejl som innehåller personuppgifter. Det är också viktigt att vi har kännedom om och kontroll över våra rutiner och att vi är transparenta kring hur vi behandlar personuppgifter. Den dokumentation du gör ska du mejla till dataskyddssamordnaren.

Tänk också på att dölja mottagarnas e-postadresser vid utskick till flera externa mottagare. Du kan läsa mer om hur du gör här.

- **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 hänvisa till Svenska Röda Korsets Dataskyddspolicy som kommer att finnas på redcross.se från och med maj 2018. Rent konkret innebär detta att vi, när personuppgifter samlas in, på något sätt behöver informera individen om hur och varför vi behandlar deras personuppgifter. I alla digitala kanaler betyder det att vi kommer att ha en kort text där vi berättar att vi behandlar deras personuppgifter och länkar till var de kan läsa mer. I de fall där vi exempelvis samlar in personuppgifter face-to-face behöver vi nämna detta tydligt och hänvisa till redcross.se där personerna kan läsa mer om hur vi kommer att behandla deras personuppgifter.

- **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. Här är det också viktigt att tänka på att inte lämna ut information genom att exempelvis berätta för vänner och bekanta om att en viss känd person har givit pengar eller liknande. Tänk också på att obehörig inte alltid behöver vara en extern person - det kan lika gärna handla om andra anställda som inte har behörighet till samma system och därigenom uppgifter som du har. Det är alltså alltid viktigt att vara försiktig och restriktiv när det gäller personuppgifter.

- **Lagring av personuppgifter:** Vi har en skyldighet att se till att inte spara personuppgifter längre än vad som är nödvändigt. Lika viktigt som det är att ha rutiner för hur vi samlar in personuppgifter, lika viktigt är det att ha rutiner för hur och när vi tar bort personuppgifter. Vi arbetar med att ta fram rutinbeskrivningar och dessa kommer att tillgängliggöras senare. Har du egna rutiner som endast du eller ett fåtal arbetar med eller känner till så är det viktigt att du skriver ner denna rutin och skickar det till dataskyddssamordnaren.

- **Molntjänster:** Utgångspunkten är att vi inte ska använda egna molntjänster, som exempelvis Google Drive och Dropbox för behandling av personuppgifter. Använd istället de tjänster vi har, exempelvis PUFF eller G. Inom vissa av våra verksamheter kan det ändå finnas ett behov av att använda egna molntjänster för att det inte finns något annat rimligt alternativ. Det är då viktigt att du dokumenterar denna rutin och skickar den till dataskyddssamordnaren.

- **Dataskyddspolicy:** Det är viktigt att du känner till vår dataskyddspolicy. Den kommer att tillgängliggöras på redcross.se och på Rednet så snart den antagits av styrelsen. Dataskyddspolicyn är ett mycket bra dokument där du på några få sidor får en tydlig bild över i vilka situationer vi samlar in och hur vi behandlar personuppgifter.