DATASKYDDSFÖRORDNINGEN

HANDBOK FÖR IDEELLA ORGANISATIONER

Framtagen av SVO
Version 1.0 maj 2018

Innehållsförteckning

Inledning

Dataskyddsförordningen (även kallad GDPR - General Data Protection Regulation) börjar gälla den 25 maj 2018. Alla företag, organisationer och myndigheter i EU-länderna berörs av den nya lagen. Din organisation kommer att behöva se över hur, vad och varför ni lagrar personuppgifter. Troligen kommer ni behöva göra vissa åtgärder för att undvika att riskera höga bötesbelopp. Förordningen införs för att stärka den enskilda individens integritet.

Samverkande Organisationer, SVO

Denna handbok är framtagen för att stötta ideella organisationer i deras arbete att anpassa verksamheten till den nya lagstiftningen.

Bakom handboken står SVO som är ett nätverk av nio stycken stora ideella organisationer (Aktiespararna, Svenska Brukshundklubben, Företagarna, Jägareförbundet, Svenska Kennelklubben, Kryssarklubben, Sportfiskarna, Skattebetalarna och Villaägarna). SVO arbetar med information, utbildning och erfarenhetsutbyte mellan sina medlemmar för att stärka en positiv organisationsutveckling. Erfarenhetsutbytet är det främsta instrumentet i det praktiska arbetet. Samverkan i SVO präglas av en öppen, konkurrensfri och generös attityd till varandra och omvärlden.

Utöver sedvanliga kvartalsmöten genomförs regelbundet andra sammankomster med olika medarbetarkategorier i SVO-organisationerna. Exempelvis har sammankomster arrangerats kring frågor om ekonomihantering och ekonomisystem, medlemsrekrytering, erfarenheter och utveckling av medlemsregister, förstärkt arbete med datasäkerhet, erfarenheter kring tidningsproduktion, olika typer av skattefrågor mm.

En stor arbetsuppgift har också varit att stötta varandra i det förberedande arbetet med införandet och anpassning av GDPR. Inte bara den handbok som du ser här, utan också olika typer av dokument som kan användas inom respektive organisation i det fortsatta GDPR-arbetet.

Syftet med handboken

Handboken ska fungera som ett komplement till texten i förordningen samt på Datainspektionens webbsida. Datainspektionen kommer fungera som tillsynsmyndighet när lagen träder i kraft.

Handboken tar upp begrepp som förekommer i förordningen, rekommendationer på vad organisationerna bör fokusera på samt checklistor och mallar som syftar till att underlätta arbetet.

Trots att GDPR snart börjar gälla är den nationella anpassningen till förordningen ännu inte klar och det förekommer en hel del frågetecken kring hur förordningen ska tillämpas. Därför beskriver handboken ett nuläge (april 2018) och syftar till att beskriva och rekommendera snarare än att tolka och leverera sanningar.

Aktuell information om GDPR finner du på:
www.datainspektionen.se

Checklista för att påbörja anpassningen till GDPR

Det svåra med GDPR är att veta var man ska börja. Datainspektionen har tagit fram ett bra underlag som hjälper till i förberedelserna. Det hittar du på Datainspektionens webbsida.

För att förenkla det ytterligare har SVO tagit fram en egen checklista.

1 Leta information

Svenska Kennelklubben har tagit fram bra material över vad ideella organisationer behöver tänka på. All information hittar du på Svenska Kennelklubbens webbsida, www.skk.se. På Datainspektionens webbsida finns det också information om den nya förordningen.

2 Utse en ansvarig

Utse en person eller grupp i organisationen som är ansvarig för att sätta sig in i frågorna och börja läsa på. Ansvarig för GDPR i organisationen kan också vara den som ser till att nya funktionärer eller förtroendevalda får information om GDPR och er hantering av den.

3 Gör en inventering av register

Genom att se över vilka personregister er organisation har, får ni en bättre överblick över hur hanteringen ser ut. Då kan ni rensa bort en del, skapa rutiner för vilka register ni ska ha och bestämma varför vissa register måste finnas. Skriv en registerförteckning så att ni vet vilka register ni har. Håll registerförteckningen uppdaterad genom att hålla nere antalet personregister och föra in eventuella nya register som skapas.

4 Se över vilka personuppgifter ni sparar och i vilket syfte

Behandling av personuppgifter ska ske på ett lagligt, korrekt och öppet sätt. Spara därför endast de personuppgifter som är nödvändiga för att kunna bedriva er verksamhet och upprätthålla en god medlemsvård. Registerförteckningen ska innehålla en formulering om hur länge ni sparar personuppgifterna samt på vilken grund ni lagrar dem. Det kan krävas olika formuleringar för olika register, beroende på syftet med lagringen. Se till att ni inte sparar fler uppgifter än vad ni behöver. Läs mer om detta på datainspektionens webbplats.

5 Se över säkerheten

Minimera risken för att personuppgifter läcker ut. Detta gör ni bäst genom att skapa rutiner för vilka som får hantera och spara register, och på vilket sätt de sparas. Se till att personuppgifter inte sparas på personers egna datorer eller andra ställen där säkerheten är låg. Det bästa är om uppgifterna ligger skyddade bakom ordentliga brandväggar. Läs mer under avsnittet *IT-säkerhet*. Självklart ska fysiska register skyddas av låsta skåp eller annan säker förvaring.

I GDPR finns en rapporteringsskyldighet vid dataintrång. Skulle personuppgifter läcka, t ex om någon mister sin dator eller telefon med personregister i eller någon hackar sig in organisationens digitala system, har ni 72 timmar på er från att det upptäcks, att

rapportera det till Datainspektionen. Det kan komma att bli aktuellt att även delge detta till de drabbade. Mer information finns under avsnittet *IT-säkerhet*.

6 Skriv personuppgiftsbiträdesavtal

Alla externa parter som ni lämnar ut personuppgifter till är era personuppgiftsbiträden som ni ska skriva ett personuppgiftsbiträdesavtal med. Det finns avtalsmallar för detta och är inte speciellt komplicerat. Avtalet klargör vilket ansvar biträdet har över era personregister och på vilket sätt de får hanteras. Det kan t.ex. vara tryckeriet som trycker er medlemstidning (och distribuerar den). Det kan också komma att bli aktuellt att instanser inom organisationen är personuppgiftsbiträden för varandra.

7 Personuppgifter i ostrukturerat material

Alla personuppgifter som förekommer i t.ex. mejl, protokoll, brev och på webbsida, så kallat ostrukturerat material, omfattas också av GDPR. Så har det inte varit tidigare. Det innebär att ni behöver undersöka att publicering av personuppgifter i ostrukturerat material har rättsligt stöd, att ni skapar rutiner för hur ni avpersonifierar uppgifter i handlingar och att ni informerar de registrerade på ett korrekt sätt. Ett utgivningsbevis gör bland annat att webbplatsen får grundlagsskydd enligt yttrandefrihetsgrundlagen. Läs mer om utgivningsbevis under rubriken *Digitala medier*.

8 Informera om hur ni hanterar personuppgifter

Den sista, och kanske viktigaste punkten, är att vara tydlig i informationen till personerna ni registrerar hur ni hanterar deras uppgifter och att ni noga motiverar hur behandlingen av dessa sker. Detta gäller inte bara när personer registrerar sig som medlemmar, utan även personuppgifter som samlas in vid t.ex. anmälan till kurser, tävlingar och andra aktiviteter samt register över funktionärer mm.

Medlemsvillkor

I organisationens medlemsvillkor ska det framgå hur personuppgifter behandlas. Dessa ska personen känna till och aktivt godkänna innan de blir medlemmar eller påbörjar en ny medlemsperiod. Det aktiva godkännandet kan ske genom att personen klickar i en ruta eller betalar din avi. Länka till medlemsvillkoren på era medlemssidor och gör klart att det är personens ansvar att ta del av dessa innan de godkänner. En sammanfattning av medlemsvillkoren, och länk till dem i sin helhet, bör finnas med i medlemsavin eller i det digitala anmälningsformuläret.

Det finns delar i medlemsvillkoren som personen kan avsäga sig. Det kan t.ex. vara att få en tidning, nyhetsbrev eller erbjudanden från samarbetspartners. Detta ska organisationen kunna tillmötesgå. Kan ni inte hantera det idag, bör era system utvecklas så det blir möjligt. Det är viktigt att även t.ex. distrikt eller föreningar ger denna möjlighet till personer gällande den egna tidningen och erbjudanden från lokala samarbetspartners.

Organisationen har inte rätt att behandla personuppgifter utöver det som står i medlemsvillkoren. Därför är det extra viktigt att medlemsvillkoren innefattar all behandling och att det efterföljs av alla personer inom och utanför organisationen som hanterar dessa personuppgifter.

Begrepp och rekommendationer för att förstå GDPR

I den här handboken kommer det förekomma en rad begrepp som är relevanta för att övergripande förstå innehållet i GDPR. Eftersom innehållet är anpassat till ideella organisationer använder vi följande begrepp för att beskriva organisations olika insatser:

Förbund - organisationens nationella instans.

Distrikt - organisationens regionala instans.

Förening - organisationens lokala instans.

Vad är en personuppgift?

Varje uppgift som kan identifiera en fysisk nu levande person, direkt eller indirekt. Namn, personnummer, adress, e-postadress och fotografi är exempel på personuppgifter.

Barns personuppgifter

Ni bör redan nu fundera på hur ni ska kontrollera en persons ålder och hur ni ska inhämta vårdnadshavares samtycke i samband med behandling av barns personuppgifter online.

Genom dataskyddsförordningen införs ett förstärkt skydd för barns personuppgifter, särskilt när det gäller kommersiella internettjänster som sociala nätverk. Kort sagt, om ni erbjuder den typen av tjänster till barn måste ni inhämta vårdnadshavares samtycke för att få behandla barnets uppgifter. Detta gäller enligt förordningen, barn under 16 år om de tjänar egna pengar som de betalar med, annars gäller det barn under 18 år. Rekommendationen blir att enligt försiktighetsprincipen ta in vårdnadshavarens samtycke på alla under 18 år. Kom ihåg att ni också måste kunna visa att vårdnadshavarens samtycke har lämnats.

Eftersom barn enligt förordningen förtjänar särskilt skydd måste all den information som riktar sig till barn vara skriven på ett tydligt och enkelt sätt som barn förstår. Barns skyddsvärda ställning ska också vägas in vid en intresseavvägning.

Läs mer om barn personuppgifter på Datainspektionens webbsida.

Känsliga personuppgifter

- Hälsa
- Etniskt ursprung
- Politiska åsikter
- Religiös/filosofisk övertygelse
- Medlemskap i fackförening
- Sexuell läggning
- Biometriska och genetiska uppgifter (t.ex. storlek på kläder).

Kvasiidentifierare

Något som kan hänföras till en enskild person utan att det är direkta personuppgifter t.ex. kommun, kön och yrke i kombination – kan hänföra till ca 260 personer och därmed går en person att identifiera.

Personuppgiftsregister (personregister)

Ett register som innehåller personuppgifter. Register med kombination av minst två personuppgifter om samma person, som kan identifiera personen ifråga anses som ett personuppgiftsregister.

Personuppgiftsansvarig

Det är den som behandlar någon annans personuppgifter (som inte sker i rent privat användning). Det är varje enskild organisation som är personuppgiftsansvarig, eftersom varje organisation är en egen juridisk person. Organisationen bär själva ansvaret för den behandling av personuppgifter som görs inom just er organisation.

Dataskyddsombud

Ombudets roll är att kontrollera att dataskyddsförordningen (GDPR) följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser. Ombudet ska vara direkt underställd ledning med uppgift att kontrollera att behandlingen utförs på ett korrekt sätt. Ombudet ska ha speciella villkor gällande uppsägning.

Enligt datainspektionen finns det idag inget krav på att ideella organisationer ska ha ett dataskyddsombud, men de rekommenderar att man ändå utser ett. Det går att ta in en extern resurs där t.ex. flera organisationer har samma ombud. Det är upp till varje enskild juridisk person, er organisation, att besluta om ni anser att ni är i behov av ett dataskyddsombud inom er organisation och i så fall utse ett dataskyddsombud.

Personuppgiftsbiträde

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Det är exempelvis samarbetspartners, myndigheter eller utomstående personer som tar del av era personuppgifter inom organisationen. Ett skriftligt avtal måste upprättas (personuppgiftsbiträdesavtal). Det är den personuppgiftsansvarige som ansvarar för att avtalet finns.

Personuppgiftsbiträdesavtal

Ett avtal som upprättas mellan den personuppgiftsansvarige och personuppgiftsbiträdet. I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktionerna och att personuppgiftsbiträdet måste vidta de säkerhetsåtgärder som den personuppgiftsansvarige ska vidta.

Principer för dataskydd

All behandling ska vara laglig, korrekt och öppen.

Begränsning

Ändamålen ska vara särskilda, uttryckligt angivna och berättigade ändamål. Varje register ska ha laglig grund och specifika ändamål. Registret ska även ha tydliga regler för hur länge det sparas och varför.

Uppgiftsminimering

Uppgifterna som behandlas och lagras ska vara adekvata, relevanta och inte för omfattande. Bara de uppgifter som behövs för att driva verksamheten får lagras och behandlas.

Lagringsminimering

Uppgifterna får inte sparas längre än nödvändigt.

Integritet och konfidentiellt

Uppgifterna ska vara skyddade och inte exponeras för obehöriga.

Ansvarsskyldighet

Den personuppgiftsansvarige ansvarar för att uppgifterna behandlas efter ovanstående principer.

Behandling av personuppgifter

Hur vi använder personuppgifter i våra register. Personer som är lagrade i register ska ha tillgång till information om hur uppgifterna används och de ska ha givit sitt aktiva medgivande till både lagring och behandling. Personuppgifterna som samlas in ska vara relevanta för ändamålet man har med behandlingen. En organisation ska därför inte samla in extra uppgifter som inte behövs om en person.

Organisationen får inte behandla personuppgifter på något annat sätt än det som framgått av informationen till den registrerade personen.

I Dataskyddsförordningen finns det också en princip som säger att personuppgifterna inte får sparas längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna har samlats in. Det innebär att er organisation inte får spara personuppgifter under längre tid än ni har laglig grund för.

Exempel på när ni använder registrerades personuppgifter kan vara vid:

- Insamling
- Registrering
- Lagring
- Bearbetning
- Spridning
- Samkörning
- Radering

Lagring

Hur organisationen lagrar personuppgifter. Organisationen måste definiera var och varför personuppgifter lagras, så kallad laglig grund. Personen ska dessutom vara underrättad om hur och varför dennes personuppgifter lagras. För varje register som upprättas ska det finnas ett motiv till varför registret sparas och hur länge uppgifterna sparas. Exempel på var organisationer lagrar personuppgifter:

- Deltagarlistor
- Medlemslistor
- Resultatlistor
- Funktionärslistor
- Prov- och tävlingssystem
- Webbsida
- Protokoll
- E-post
- Molntjänster – Google drive, OneDrive; Dropbox etc.

Laglig grund

All lagring av personuppgifter måste följa förordningen. Beroende på registrets syfte och karaktär kan den lagliga grunden variera.

Samtycke

En person ska frivilligt kunna samtycka till hur personuppgifterna behandlas efter att den registrerade har fått information om personuppgiftsbehandlingen. Samtycket ska, otvetydigt, genom en aktiv handling, lämnas av personen för att organisationen ska få använda uppgifterna i specifika situationer. Den som behandlar personuppgifter med stöd av ett samtycke måste kunna visa att ett giltigt samtycke har lämnats av den registrerade. Ett samtycke ska närsomhelst kunna återkallas av den registrerade lika lätt som det lämnades.

Avtal

Den överenskommelse som organisation och personen ingår när exempelvis en medlemsavgift betalas in. Den behandling av personuppgifter som är nödvändig för att fullgöra avtalet ska tydligt definieras i medlemsvillkoren och finnas lättillgängligt för personen att ta del av. I avtalet ingår behandling av personuppgifter som är nödvändiga för att avtalet ska kunna efterföljas. Personuppgiftsbehandling i enlighet med avtalet kan inte personen avsäga sig utan att samtidigt bryta avtalet.

Rättslig förpliktelse

Personuppgifter får behandlas om det är nödvändigt för att uppfylla en rättslig förpliktelse. Som exempel på en rättslig förpliktelse kan nämnas bokföringsskyldigheten som anges i bokföringslagen.

Berättigat intresse/intresseavvägning

Behandling av personuppgifter där organisationens intresse väger tyngre än den registrerades intresse av skydd för sina personuppgifter. Barn anses vara särskilt skyddsvärda. T.ex. när organisationen lämnar ut uppgifter till samarbetspartners i syfte att informera medlemmen om dess förmåner eller erbjudanden.

Om den registrerade personen invänder mot en pågående behandling måste organisationen göra en ny intresseavvägning och upphöra med behandlingen om det inte finns tillräckliga belägg för att fortsätta behandlingen. Om personen invänder mot behandling som sker för direkt marknadsföring måste behandlingen upphöra.

Registrerade personers rättigheter

Rätt till information

Registrerad person har rätt att få information när dennes personuppgifter behandlas. Bland annat ska information lämnas om kontaktuppgifter till den personuppgiftsansvarige, den rättsliga grunden för behandlingen och ändamålet med behandlingen.

Information ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) och det finns risk för till exempel identitetsstöld eller bedrägeri.

Rätten att bli glömd

En registrerad person har rätt att få sina uppgifter borttagna. Om det finns annan lagstiftning som kräver att uppgifterna sparas kan de dock inte raderas. Det kan även förekomma en intresseavvägning då organisationen ändå kan spara uppgifter utan personens samtycke. Det kan också hända att organisationens intresse för att spara uppgifterna väger tyngre än den registrerades önskan att få desamma raderade. Till exempel om någon som är utesluten vill bli raderad/glömd. Då kan organisationens intresse av att ha kvar uppgifterna väga tyngre, d.v.s. organisationen måste ha kvar informationen om att personen är utesluten, för att denne inte ska kunna bli medlem igen. Detta kan även appliceras på protokoll från möten och sammanträden vilka är en förutsättning för demokratiska organisationer. Då skulle man kunna göra bedömningen att organisationen har berättigat intresse. På samma sätt som man kan anse att registrerade, och även publicerade, tävlingsresultat är en förutsättning för tävlingar.

Det är viktigt att organisationen endast lagrar/publicerar relevanta personuppgifter för ändamålet samt att till exempel protokoll skrivs sakligt och utan onödiga personuppgifter eller utlämnade information.

Rätt till korrigering

Organisation måste korrigera felaktiga uppgifter på begäran av den registrerade.

Rätt till dataportabilitet

Den registrerade personen har rätt att få sina uppgifter flyttade. Uppgifterna ska då göras tillgängliga i en fil i digitalt format som kan läsas av vanliga system, t.ex. xml.

Rätt att få ut sina uppgifter som behandlats

Registrerad person har rätt att kostnadsfritt en gång om året få ett utdrag på all behandling av dennes personuppgifter. Detta gäller såväl digitala som analoga register. Informationen ska tillhandahållas i en lättillgänglig, skriftlig form och med ett tydligt och enkelt språk.

Rätt att begränsa direktmarknadsföring

Registrerad person har rätt att begränsa vilka personuppgifter som behandlas av företag med syfte till riktad, personifierad marknadsföring.

Medlemsvillkor

Den information som beskriver för den registrerade personen hur organisationen behandlar och lagrar personuppgifter. Medlemsvillkoren ska formuleras med ett tydligt och enkelt språk och ska vara lättillgängligt. Information om medlemsvillkoren ska den registrerade kunna ta del av innan denne beslutar att ingå avtal med organisationen eller lämnar sitt samtycke.

Missbruksregel

Missbruksregeln innebar tidigare att man kunde använda enklare regler för personuppgifter i ostrukturerat material (på hemsidor, e-post, enkla dokument osv). I GDPR finns ingen sådan regel varför ostrukturerat material lyder under samma lagliga grund som all annan behandling.

Personuppgiftsincident

Om det inträffar en säkerhetsincident som rör personuppgifter, till exempel ett dataintrång eller en oavsiktlig förlust av personuppgifter.

Rapporteringsskyldighet

När man upptäcker en personuppgiftsincident måste man dokumentera incidenten och anmäla den till Datainspektionen inom 72 timmar. Man kan också behöva informera de registrerade, till exempel om det finns risk för id-stöld eller bedrägeri.

Vite

Datainspektionen är tillsynsmyndighet för GDPR. Det är alltså den myndighet som ska se till att GDPR efterföljs. Företag, organisationer och myndigheter som inte uppfyller kraven i GDPR riskerar ett stort vite på upp till 20 miljoner euro alternativt 4 procent av den globala årsomsättningen.

Privacy by design

Begrepp för att nya system har inbyggt systemstöd för GDPR.

Code of conduct

Uppförandekoder inom varje bransch som kommer sätta standarden för tillämpningen av GDPR. Att ta del av utfall av domstolsbeslut kan vara ett sätt att sätta standarden.

Digitala medier

Webbsida

Utgivningsbevis ger grundlagsskydd

Ett utgivningsbevis innebär att webbplatsen får grundlagsskydd enligt yttrandefrihetsgrundlagen. Grundlagsskyddet gör att reglerna i dataskyddsförordningen inte gäller och då är det tillåtet att publicera personuppgifter som till exempel namn och adress utan att organisationen behöver personens tillåtelse.

Det krävs en del specifika förutsättningar för att få utgivningsbevis. Mer om detta finns på Myndigheten för press, radio och tv:s webbplats www.mprt.se.

Skyldigheter

Om du får ett utgivningsbevis för en databas eller webbplats så har du vissa skyldigheter.

- En utgivare ska alltid finnas. Han eller hon har ensam det straffrättsliga ansvaret för vad som publiceras. Läs mer på Myndigheten för press, radio och tv:s webbsida: www.mprt.se/att-sanda/krav-och-regler/ansvarig-utgivare
- Webbplatsens och utgivarens namn samt vem som har utsett utgivaren ska publiceras på webbplatsen.
- Innehållet på webbplatsen ska dokumenteras i sex månader.

Skyldigheterna påverkar inte grundlagsskyddet men är i de flesta fallen straffsanktionerade.

Sociala medier – ansvar och att tänka på

Använder ni er av sociala medier, ex. Facebook eller Instagram så har ni också ansvar för de personuppgifter ni hanterar på den sidan eller plattformen. Framförallt bör ni se över vad för inlägg och bilder ni lägger ut på er plattform, eftersom ni troligtvis hanterar någons personuppgifter. Skulle ni dessutom publicera en bild på en person med exempelvis en bruten arm eller liknande – så har ni inte bara behandlat någons personuppgifter utan även dennes känsliga personuppgifter (hälsa).

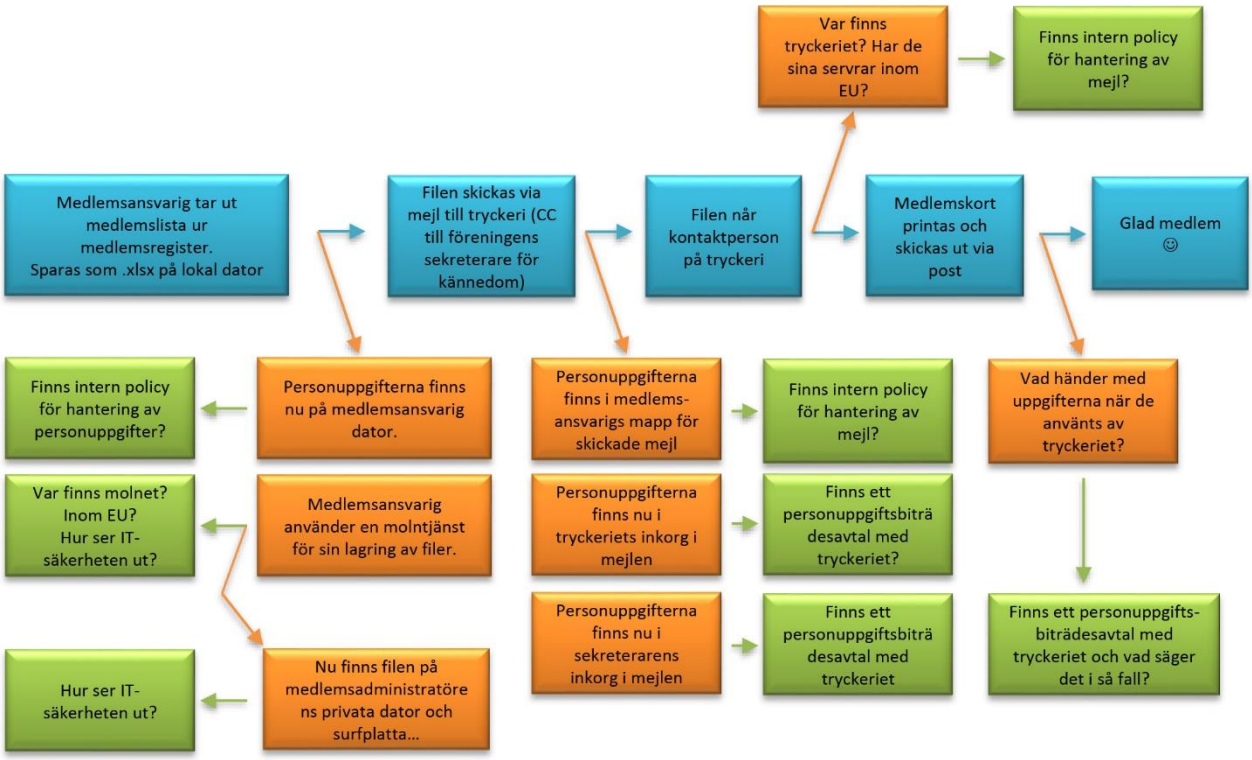
Skulle en person kommentera ett inlägg så behandlar ni automatiskt den personens personuppgifter. Troligtvis kan dock denne personen självt ha ansetts godkänt er behandling av personuppgifter eftersom denne självmant valt att kommentera inlägget. Skulle det dock vara så att en person i sin kommentar nämner en tredje person vid namn blir det dock tveksamt om ni har rätt att behandla denna personens uppgifter. Då krävs det att ni går in och raderar kommentaren eller personuppgifterna som ni inte har laglig grund för.

IT-Säkerhet

Eftersom GDPR sätter höga krav på hantering av personuppgifter och på vilket sätt de lagras, behöver ni tänka över ert sätt att arbeta med IT-säkerheten. Eftersom de allra flesta personuppgifter idag sparas digitalt, handlar mycket av anpassningen om att ha system som uppfyller alla krav. Det gäller också att ställa krav och kontrollera leverantörer, och andra aktörer som behandlar personuppgifter åt er, så att de följer GDPR. Skapa rutiner för hur ni snabbt kan agera om ni till exempel får ett intrång eller om en medlem begär att få ut sina uppgifter, eller vill bli glömd. Rutinerna kan antingen vara automatiska eller manuella.

Exempel på ett flödesschema

En exemplifiering hur personuppgifter sprider sig och hur man kan arbeta för att säkerställa organisationens behandling av personuppgifter.



Backup

Varför tar man backup?

För att säkerställa data och kunna återskapa till specifikt läge. Inför GDPR behöver ni ha gått igenom och dokumenterat era backup-rutiner. Tänk då även på hur viktig informationen är för er. Ställ er följande frågor:

- Vilken skada skulle det ge er och andra om den inte skulle kunna återställas?
- Hur skulle det gå om ni inte kan återställa förlorad information?
- Kan ni återställa informationen på annat sätt, exempelvis papperskopior?

Vilken information bör sparas?
Fråga er vad som är viktigt för er verksamhet och historiken kring den. Utifrån det, sätt upp rutiner för hur backuper ska göras. Det som ni anser inte är viktigt, ta inte med det i backuperna.

På vilken utrustning tar ni backuper?

- Servrar
- Workstations
- Laptops
- Plattor
- Telefoner

Hur länge spar ni er backupdata?
GDPR omfattar även backuper. Se över vilken laglig grund ni har till era olika register och anpassa backupen efter det. Det kan vara olika för olika register. Vanligast är att ha daglig/vecko/månads samt årsbackuper. Utgå ifrån hur mycket data som förändras dagligen i ert system. Glöm inte att testa återställningsfunktionen regelbundet.

Vilka har tillgång till er backup-data?
Fundera kring var backuperna sparas. Är det internt, externt eller i molnet? Kartlägg hur fördelningen ser ut och se till att behörigheten till dessa är dokumenterad och begränsad. Är det externa aktörer som sparar er data med personuppgifter – skriv ett personuppgiftsbiträdesavtal som reglerar hur hanteringen ska se ut. Säkerställ också att ni kommer åt er data när den ska återställas.

Utse en huvudansvarig och en reserv.

Rättigheter kring personuppgifter i backuper
Eftersom GDPR ger registrerade personer rätt att, på begäran, få ut uppgifter om var dennes personuppgifter finns lagrade, behöver ni ha en rutin för hur ni tar ut detta från era backuper. Här är det noga att rensa personuppgifter från backuperna så att de inte ligger lagrade för länge. Gör samma sak för den registrerades rätt att bli glömd.

Systemöversikt
Se till att ni gör en systemöversikt som dokumenteras så att flera kan ta del av det. Genom systemöversikten får ni bättre kontroll över era personuppgifter och kan agera snabbare om något inträffar.

Mejl
Ni bör skapa en mejlhanteringspolicy som alla ska följa. Kartlägg hur ni hanterar mejl, hur ni hanterar delade mejlboxar, var mejltjänsten finns lagrad, hur ofta ni ska tömma såväl inkorg som skickat-mappen samt papperskorg.
För aktuell information om mejlhantering se Datainspektionens webbsida.

Moln
Om ni använder lagringsplats i molnet, ta reda på var den är lokaliserad. Beroende på om den är lokaliserad inom eller utanför EU gäller olika regler.

Ta reda på vem som äger/säljer tjänsten, ställ krav på att de följer GDPR och skriv personuppgiftsbiträdesavtal om det krävs. Se också över hur ni styr behörigheter.

Intranät
I ert intranät är det lika viktigt att ha kontroll på personuppgifterna som på den publika webben. Kartlägg var servrarna ligger, internt eller externt. Se vilka som kommer åt dem fysiskt och vilka som är administratörer och redaktörer, alltså de som påverkar innehållet

på intranätet. Var noga med att styra behörigheten så att inte obehöriga har tillgång, till exempel före detta anställda eller andra administratörer. Dokumentera vem som är ansvarig för drift och innehåll. Kartlägg vilka arbetsstationer som kommer åt intranätet och se till att de är säkra.

Datorer

Datorer är en mycket viktig del i systemöversikten eftersom de är många som är kopplade till samma nätverk. Här är det viktigt att styra behörigheter så att användaren är begränsad i sin åtkomst. Sätt upp rutiner för hur användaren ska sköta säkerheten över sin egen dator. Ta policybeslut rörande hur användaren ska agera om datorn följer med hem, används på publika nätverk, där risken för intrång är större, och vad användaren måste göra om datorn försvinner.

Ha automatiskt skärmlås på samtliga datorer samt kräv inloggning för att obehöriga inte ska komma åt information som kan vara känslig. Ha en lösenordspolicy där ni bestämmer komplexitet på lösenorden, hur ofta de ska bytas och om ytterligare säkerhet behövs kring de delar på datorn och i nätverket som hanterar personuppgifter. Observera att webbläsaren ofta kan spara inloggningsuppgifterna för enklarare inloggning. Detta skapar en stor säkerhetsrisk då obehöriga kan logga in utan att veta koder eller användarnamn.

Hantering av upptäckt intrång

Enligt GDPR är ni rapportskyldiga om det sker ett intrång hos er där det finns risk att personuppgifter har läckt ut. Inom 72 timmar från det att ni upptäcker intrång, ska det rapporteras till Datainspektionen. Det kan också var aktuellt att ni ska informera de personer som ni misstänker har drabbats.

Försök att förbered er så mycket som möjligt inför ett intrång så ni kan handla snabbt om det väl händer. Ta fram en rapportmall för att förenkla arbetet. Skapa rutiner och checklistor för vad ni ska göra när ett intrång sker och informera de ansvariga.

Nätverket

Precis som med alla andra delar i systemöversikten behöver ni se över ert nätverk. Kartlägg hur lösningen ser ut, vilka leverantörer ni har och säkerställ att er lokala data inte har obehörig åtkomst.

Trådlösa nätverk

Se till att ha lösenordskyddat nätverk och ha separata nätverk för anställda och gäster, annars kan obehöriga ganska enkelt ta sig in i era datorer eller servrar.

Trådbundet nätverk

Bestäm om externas datorer ska få tillgång till nätverket om den pluggas i uttagen i lokalen eller om det bara får vara registrerade datorer. Genom att inte släppa in externas datorer i det trådbundna nätverket höjer ni säkerheten.

Hantera registrerade

Information till registrerade personer
Personer vars personuppgifter ni behandlar har ett antal rättigheter enligt GDPR. Rättigheterna innebär att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade, samt att få ut eller flytta sina uppgifter. De registrerades rättigheter har utökats, förstärks och specificerats i GDPR jämfört med personuppgiftslagen.

Rättelse av uppgift
Rätt till rättelse innebär enkelt förklarat att en person kan be er organisation om att få felaktiga uppgifter rättade. Personen har också rätt att få lägga till personuppgifter. Läs mer om rätt till rättelse på Datainspektionens webbplats.

Personnummer
Dataskyddsförordningen ger medlemsländerna möjlighet att bestämma villkor för hur nationella identifieringsnummer, det vill säga personnummer, får behandlas. I Sverige har det föreslagits att personnummer får behandlas om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Vidare måste övriga grundläggande principer och regler om rättslig grund uppfyllas vid behandlade av personnummer.

Känsliga personuppgifter
Alla uppgifter som enligt Dataskyddsförordningen räknas som känsliga personuppgifter är uppgifter gällande en persons:

- Hälsa,
- Etniskt ursprung,
- Politiska åsikter,
- Religiös/filosofisk övertygelse,
- Medlemskap i fackförening,
- Sexuell läggning,
- Biometriska och genetiska uppgifter (t.ex. storlek på kläder)

Känsliga personuppgifter får endast behandlas om det krävs enligt en författning (ex. inom arbetsrätt eller hälso- och sjukvård) eller om individen själv har samtyckt till det. Det är därför viktigt att ni ser över vilka personuppgifter ni hanterar och om någon av dessa är känsliga personuppgifter, ex. allergier, hälsotillstånd, storlek på kläder, fackanslutna osv.

Junior/barn
Vid erbjudande av tjänster till barn så säger Dataskyddsförordningen att det kan krävas vårdnadshavarens samtycke om barnet är under 16 år. Här har EU:s medlemsländer getts utrymme att själva bestämma åldersgränsen inom intervallet 13–16 år. Sverige har i en utredning som kom i maj 2017 gett förslag att åldersgränsen ska vara 13 år i Sverige. Ett barn som är 13 år eller äldre kan därför själv samtycka till personuppgiftsbehandling, utan en vårdnadshavares samtycke. Om barnet ska ingå ett avtal krävs dock ett medgivande från vårdnadshavaren för att det ska anses som giltigt.