RIKTLINJER FÖR GDPR

Anpassade riktlinjer för Svenska FN-förbundets distrikt och föreningar
Maj 2018

Innehåll:

UNITED NATIONS ASSOCIATION OF SWEDEN

Postadress Svenska FN-förbundet, Box 15115, 104 65 Stockholm • *Besöksadress* Skolgränd 2 • *Telefon* 08-462 25 40 • *Fax* 08-641 88 76 • *E-post* info@fn.se • *Webb* www.fn.se

Address United Nations Association of Sweden, P.O. Box 15115, SE-104 65 Stockholm, Sweden • *Phone* +46-8-462 25 40 • *Fax* +46-8-641 88 76 • *E-mail* info@fn.se

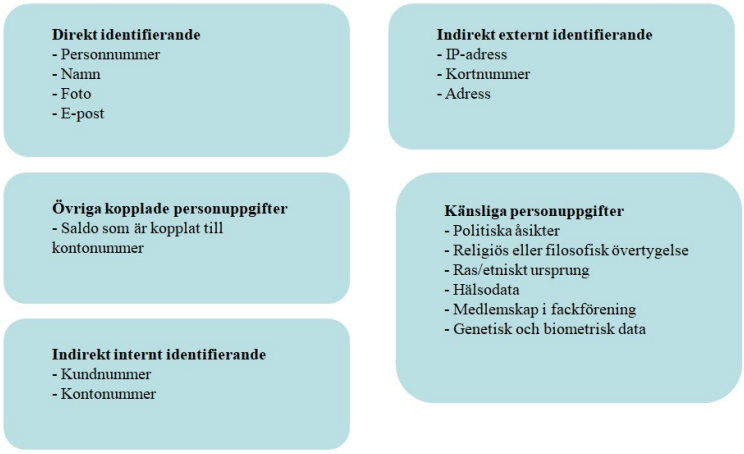
GRUNDLÄGGANDE OM GDPR

En ny Dataskyddsförordning, även kallad General Data Protection Regulation (GDPR), träder i kraft 25 maj 2018. Förordningen ersätter Personuppgiftslagen (PUL) som har gällt tidigare i Sverige. Syftet med förordningen är dels att skydda privatpersoner vid behandling av personuppgifter, dels att möjliggöra det fria flödet av sådana uppgifter.

Med andra ord: Förordningen ska både säkerställa en hög skyddsnivå för personuppgifter och underlätta för företag och andra organisationer att använda sig av personuppgifter.

Vilka är de grundläggande principerna?
Den allra mest grundläggande principen är naturligtvis att värna om den personliga integriteten. Att hantera personuppgifter på ett korrekt och säkert sätt, så att de som anförtror oss sina uppgifter kan vara trygga. Sett ur det perspektivet blir Dataskyddsförordningen ett stöd för oss. Syftet med förordningen är dels att skydda privatpersoner vid behandling av personuppgifter, dels att möjliggöra det fria flödet av sådana uppgifter.

Vad är en personuppgift?
Personuppgifter är all slags information som direkt eller indirekt går att hänföra till en fysisk person som är i livet. Några exempel är namn, personnummer, kön, adress, telefonnummer, e-postadress, kontonummer, bilder och ljudupptagningar samt cookie-id, ip-adress eller andra elektroniska identifierare. Nedan ser en bild på olika kategorier av personuppgifter.



Vem ansvarar för vad?
Personuppgiftsansvarig är organisationen, den juridiska personen, den som bestämmer ändamål och medel för behandlingarna av personuppgifter. Det är ytterst en uppgift för organisationens styrelse att försäkra sig om att kraven enligt förordningen är uppfyllda.

I Svenska FN-förbundets fall har riksförening, distrikt och lokalföreningar ett gemensamt ansvar för vissa uppgifter om medlemmarna. Detta gäller den information som finns i vårt CRM-verktyg Mysoft (det är i detta system Medlemsportalen finns). Det är viktigt att alltid ha korrekt information i Medlemsportalen, då det är där personuppgifterna för våra medlemmar finns.

OBS! Viktigt att komma ihåg är att respektive distrikt och förening utöver det gemensamma ansvaret har eget ansvar för alla andra personuppgifter.

REKOMMENDATIONER TILL FÖRENINGAR OCH DISTRIKT

För att behandla personuppgifter är våra rekommendationer att ni gör följande:
(Under avsnitt ”FÖRDJUPNING OM GDPR” finns en fördjupning kring varje punkt).

1. *GDPR på agendan*
2. *Översyn av personuppgifter*
3. *Ändamål*
4. *Översyn av leverantörer och kontakter*
5. *Uppgiftshantering*
6. *Individens rättigheter*
7. *Säkerhet*
8. *Ansvar*

1. GDPR på agendan (fördjupning sid 6)
Vad säger GDPR: Det är ytterst en uppgift för organisationens styrelse att försäkra sig om att kraven enligt förordningen är uppfyllda.

Att tänka på:

- Klarlägg att detta är en strategisk fråga som styrelsen ytterst är ansvarig för.
- Klarlägg ansvarsförhållanden. Vad är vår organisation ansvarig för? Vad har vi tillsammans med andra ett gemensamt ansvar för?
- Informera och utbilda alla som behandlar personuppgifter, för att etablera goda rutiner.
- Bestäm vem eller vilka som ska ha den uttalade uppgiften att upprätta ett behandlingsregister.
- Se över vilka förändringar som behöver göras. Ta fram en integritetspolicy.

OBS! Viktigt att tänka på är att föreningar och distrikt, som är egna juridiska personer, inte kan referera vidare till riksföreningens generella information och policy. Däremot går det att hämta inspiration från riksföreningen.

---

2. Översyn av personuppgifter (fördjupning sid 6)
Vad säger GDPR: Att vi behandlar uppgifter endast om vi har rättsliga grunder för det och att vi är transparenta gentemot de registrerade.

Att tänka på:

- Kartlägg vilka behandlingar av personuppgifter ni har. Ett angreppssätt kan vara att utgå från vilka kategorier av personer ni behandlar uppgifter om. Ett annat sätt kan vara att utgå från de system ni använder för behandlingar av personuppgifter. I kartläggningen av personuppgifter bör innehålla följande delar:
  - Vem = Vilka olika grupper av personer som förekommer som registrerade.
  - Vad = Vilka olika behandlingar av personuppgifter som sker för dessa grupper av personer.
  - Varför = Beskrivning av ändamål (varför personuppgiften sparas) för varje enskild behandling och fastställ den rättsliga grunden för varje enskild behandling.
  - Varför = Beskriv hur ni fått tillgång till uppgiften, vart de finns och hur länge ni sparar dem.
  - Vem = Beskriv vem som har tillgång till uppgifterna.
  - Hur = Beskriv hur ni hanterar säkerheten kring personuppgifterna.

---

3. Ändamål (fördjupning sid 7)
Vad säger GDPR: Att vi behandlar uppgifter endast för uttryckligt angivna och berättigade ändamål och att vi inte ändrar på definitionerna av ändamålen i efterhand. De rättsliga grunderna är:

- Avtalsförhållande som grund går att hänvisa till hur och när detta avtalsförhållande uppstod.
- Lagkrav som grund går att hänvisa till den aktuella lagen.
- Intresseavvägning som grund ska verksamheten ha beskrivit hur den har kommit fram till att dess intressen väger tyngre än de registrerades intressen.
- Samtycke som grund ska det vara dokumenterat hur samtycke har blivit inhämtat.

Att tänka på:

- Se över era ändamål gör att spara personuppgifter enligt de rättsliga grunderna och beskriv dessa i kartläggningen.
- Ändamålen ska kommuniceras till personen när personen begär det.
- Personuppgifterna får inte behandlas för andra ändamål än det som angivits. Om ändamålet ändras måste givaren informeras.

---

4. Översyn av leverantörer och kontakter (fördjupning sid 9)
Vad säger GDPR: En viktig del i ett biträdesavtal är att biträdet endast får behandla personuppgifter enligt dokumenterade instruktioner från den ansvariga. Biträdet ska ge garantier för korrekthet och säkerhet i samband med uppdraget att behandla uppgifter för den ansvarigas räkning.

Att tänka på:

- Kartlägg vilka biträden som förekommer. Vilka tjänsteleverantörer anlitas? Har vi biträdesavtal? Granska biträdens allmänna villkor och integritetspolicys?
- Kartlägg vilka andra externa tredje parter som förekommer. Lämnas uppgifter ut till andra? Varför? Är det förenligt med de ändamål vi definierat? Vet vi att mottagande parterna hanterar uppgifterna korrekt och säkert?

---

5. Uppgiftshantering (fördjupning sid 9)
Vad säger GDPR: Att vi behandlar endast sådana uppgifter som är relevanta för ändamålen. Att vi behandlar uppgifter endast under så lång tid som är nödvändigt.

Att tänka på:

- Skapa rutiner för hur personuppgifterna uppdateras (rättas eller raderas) på ett systematiskt och kontinuerligt sätt.

---

6. Individens rättigheter (fördjupning sid 10)
Vad säger GDPR: De registrerade personerna har rätt till klar och tydlig information om vilka uppgifter om dem som vi behandlar. En registrerad person har enligt förordningen rätt att begära registerutdrag, på enkelt sätt och med rimliga intervall. Praxis för ”rimliga intervall” är en gång per år. Den registrerade ska få registerutdraget inom en månad från det att begäran inkom.

Att tänka på:

- Beskriv tydligt hur ni gör om en person begär ett registerutdrag.

OBS! Om den som begär ett registerutdrag från en lokalförening eller ett distrikt, är medlem be personen kontaktar Svenska FN-förbundet på 08-462 25 40 eller info@fn.se

---

7. Säkerhet (fördjupning sid 11)
Vad säger GDPR: Att vi ser till att hålla uppgifter uppdaterade och ser till att de inte blir manipulerade eller förstörda. Vid en personuppgiftsincident ska den ansvariga inom högst 72 timmar anmäla det till tillsynsmyndigheten Datainspektionen. Vid en allvarlig incident ska även de registrerade personerna få information om det inträffade.

Att tänka på:
- Se över er säkerhet och gör en bedömning av era risker.
- Kartlägg hur ni gör vid en incident.

8. Ansvar
Vad säger GDPR: Det är viktigt att kunna påvisa efterlevnad.

Att tänka på:
- Dokumentera tydligt hur ni arbetar med GDPR.

VARDAGSTIPS KRING GDPR

Tre faktorer för framgång med GDPR
1. TRANSPARENS - var transparenta med hur ni behandlar personuppgifter.
2. RENSA - lagra inte uppgifterna längre än nödvändigt.
3. RESPEKT - behandla endast personuppgifter ni behöver.

Samma källa
Sträva efter att samla alla personuppgifter i vårt medlemsregister (Mysoft/Medlemsportalen). Du bör helst inte ha separat lista för exempelvis medlemmarnas e-postadresser, utan se istället till att hålla telefonnummer och e-postadresser uppdaterade i medlemsregistret.

Samla in information om t ex kursdeltagare (kostvanor)
Var tydlig med vilket ändamål ni vill samla in informationen till och varför. Efter avslutat event rensa och radera de uppgifter som ej är relevanta.

Känslig information (hälsotillstånd m.m.)
Undvik att samla in känslig information så som hälsotillstånd, politisk tillhörighet m.m. då detta kräver samtycke (godkännande av personen genom aktiv handling). Finns det ändå behov av att ha denna information (exempelvis vid kurs/läger) inhämta samtycke och var tydlig med varför ni samlar in information och radera den efter avslutad aktivitet. Alternativ spara på papper och kasta efter att kurs/läger är slut.

Skicka e-post till grupper
Vid utskick av e-post till flera personer tänk på att alltid lägga in samtliga personer som dold kopia så sprider du inga personuppgifter.

En person lämnar uppgifter om en annan
Säkerställt att personen är informerad om att uppgifterna är inlämnade av inlämnare.

Under 18
För individer under 18 år krävs samtycke och godkännande av förälder. Så insamling av personuppgifter för de under 18 kräver två steg. Barnet måste veta om vad de ger in sig på (1) och föräldern måste godkänna (2) och et är först när de godkänt som det börjar gälla.

FÖRDJUPNING OM GDPR

1. **GDPR på agendan**

Personuppgiftsansvarig är organisationen, den juridiska personen, den som bestämmer ändamål och medel för behandlingarna av personuppgifter. Det är ytterst en uppgift för organisationens styrelse att försäkra sig om att kraven enligt förordningen är uppfyllda.

Dataskydd som standard

Begreppet ”dataskydd som standard” är värt att påminna om igen. Vi ska beakta dataskyddsfrågor när vi förändrar våra rutiner eller när vi utvecklar eller upphandlar nya tjänster med mera.

En viktig del i arbetet med dataskyddsfrågor är att diskutera dem internt och att öka medvetenheten. Policydokument med mera måste bli granskade åtminstone årligen och vid behov reviderade. Nya eller ändrade styrdokument måste vara förankrade och kommunicerade till alla inom organisationen som hanterar personuppgifter. En annan viktig sak att tänka på är att lägga upp en långsiktig plan för att steg för steg öka efterlevnaden av Dataskyddsförordningen.

Integritetspolicy

Det är lämpligt att ta fram en övergripande policy för organisationens hantering av personuppgifter, en integritetspolicy. En sådan policy ska beskriva vilka grundprinciper vi har för våra behandlingar av personuppgifter. Dessa grundprinciper kan mycket väl vara ordnade enligt samma struktur som Dataskyddsförordningens grundprinciper. Vi ska ju på tydligast möjliga sätt påvisa att vi efterlever förordningen.

Integritetspolicyn kan fungera som utgångspunkt för att uppdatera arbetsordningar och rutiner, för att säkerställa att vi arbetar på ett sätt som överensstämmer med det policyn utlovar. Den kan naturligtvis också ha en extern funktion, för att berätta för de registrerade vad de har rätt att förvänta sig av oss med avseende på en trygg och säker hantering av personuppgifter.

Svenska FN-förbundet har nyligen uppdaterat sin integritetspolicy och publicerat den på sidan fn.se/integritetspolicy/

OBS! **Viktigt att tänka på är att ett distrikt eller en lokalförening inte kan referera vidare till riksföreningens generella information och policy. Distrikt och lokalföreningar är egna juridiska personer.**

Däremot kan de givetvis hämta inspiration från riksföreningen om de vill upprätta sina egna motsvarande webbsidor och policydokument.

Policyer och andra styrdokument behöver inte nödvändigtvis vara publikt tillgängliga. Ibland kan räcka med att lämna ut kopior av dem när någon efterfrågar dem.

2. **Översyn av personuppgifter**

Personuppgiftsansvarig är organisationen, den juridiska personen, den som bestämmer ändamål och medel för behandlingarna av personuppgifter. Det är ytterst en uppgift för organisationens styrelse att försäkra sig om att kraven enligt förordningen är uppfyllda.

Vid kartläggningen av hur organisationen behandlar personuppgifter och vid upprättandet av behandlingsregistret är det viktigt att komma ihåg att det som ska bli beskrivet är vad som sker på kategorinivå. Det är inte varje enskild personuppgift som ska bli dokumenterad utan de typer av uppgifter organisationen behandlar om grupper av personer.

De registrerade ska vara beskrivna på gruppnivå, utifrån den roll personerna har i samband med en viss behandling. Några exempel är medlem, ambassadörer, leverantör, samarbetspartner och anställd.

Att göra en kartläggning av behandlingsregistret
Enligt Dataskyddsförordningen ska varje personuppgiftsansvarig upprätta en förteckning över sina behandlingar av personuppgifter, ett behandlingsregister.

Behandlingsregistret ska vara ett i högsta grad levande dokument. Tillkommer nya behandlingar, nya eller ändrade ändamål, nya grupper av registrerade, nya typer av uppgifter om de registrerade och så vidare, då ska vi uppdatera vårt behandlingsregister.

Vid en kartläggning bör följande områden vara med:

1. Om tillämpliga regler, ansvarsförhållanden med mera. Här ställer vi oss frågor om eventuella andra lagar att ta hänsyn till, om ansvarsfördelningen, om vi anlitar biträden och om vi lämnar ut uppgifter till andra.
2. Varför vi behandlar dessa personuppgifter. Här ställer vi oss frågor om vilken grupp av personer som är berörd, om vilket ändamål vi har och om vad som utgör den rättsliga grunden.
3. De uppgifter vi behandlar. Här ställer vi oss frågor om vilka typer av uppgifter som förekommer och om det förekommer personnummer eller känsliga uppgifter, samt från vilka källor uppgifterna kommer och hur länge vi kommer att behandla uppgifterna.
4. Hur vi behandlar uppgifterna (särskilt med avseende på integritet och konfidentialitet). Här ställer vi oss frågor om såväl tekniska lösningar som manuella rutiner, samt om hur vi hanterar incidenter.
5. Vår information till de registrerade. Här ställer vi oss frågor om när och hur vi lämnar information och om vilken information vi lämnar.

Det är viktigt att inte fastna i detaljer vid kartläggningen. Om vi börjar med de övergripande beskrivningarna kan vi alltid återkomma till dem senare och vid behov förtydliga dem på detaljnivå. Om vi identifierar problem bör vi inte försöka lösa dem direkt utan vänta till dess vi har hela bilden klar för oss och kan prioritera mellan olika problem att lösa.

För att sammanställa svaren på frågorna kan vara bra att använda ett kalkylblad. Särskilt om vi har ett stort antal behandlingar att kartlägga. En fördel med till exempel en Excel-tabell är också att det går lätt att sortera och gruppera informationen.

En mindre organisation behöver knappast skaffa sig ett mer strukturerat verktyg eller en databas för att upprätta sitt behandlingsregister. Bra att veta är dock att det existerar ett flertal verktyg på marknaden, varav många har reducerade priser för ideella organisationer.

Förordningens formkrav på behandlingsregistret är att det ska vara upprättat skriftligen, inbegripet i elektronisk form. Om det fungerar med ett register på papper som vi håller uppdaterat manuellt, då kan det vara en fullt acceptabel lösning.

3. Ändamål

Här är det viktigt att beskriva vad behandlingen syftar till, att svara på frågan ”Varför?”. En vanlig fallgrop är nämligen att många på denna punkt istället besvarar frågan ”Hur?”, vad som sker rent praktiskt med uppgifterna. Varje fortsatt behandling av samma mängd uppgifter ska vara förenlig med det ursprungliga ändamålet. Om så inte är fallet är det fråga om en ny behandling som ska bli dokumenterad separat. Ändamålet ska naturligtvis också vara legitimt, på så vis att det ska ha en rättslig grund som stöd.

Rättslig grund
Den rättsliga grunden för att behandla uppgifter om en viss grupp av personer för ett visst ändamål ska vara dokumenterad. Den dokumentationen kan se olika ut för olika rättsliga grunder.

- Är det med avtalsförhållande som grund går att hänvisa till hur och när detta avtalsförhållande uppstod.

- Är det med lagkrav som grund går att hänvisa till den aktuella lagen.
- Är det med intresseavvägning som grund ska verksamheten ha beskrivit hur den har kommit fram till att dess intressen väger tyngre än de registrerades intressen.
- Är det med samtycke som grund ska det vara dokumenterat hur samtycke har blivit inhämtat.

Den vanligast förekommande rättsliga grunden i en medlemsorganisation bör vara det avtalsförhållande som råder mellan förening och medlem. Föreningen behöver behandla uppgifter om medlemmarna för att kunna fullgöra de åtaganden som är kopplade till medlemskapet.

Även gentemot en organisations kunder och leverantörer är det avtalen med dem som utgör de rättsliga grunderna för att behandla deras uppgifter. Även om avtal är tecknade med juridiska personer så förekommer uppgifter om deras fysiska kontaktpersoner.

Den ”behändigaste” rättsliga grunden är om en organisation är tvungen enligt lag att behandla personuppgifter. Det gäller för vissa uppgifter om anställda, till exempel för att redovisa skatter och sociala avgifter eller för att leva upp till arbetsmiljölagstiftningen. För den ekonomiska redovisningen anger Bokföringslagen att uppgifter om affärshändelser ska vara sparade i minst sju år.

En situation där intresseavvägning blir aktuell är om en förening vill behandla uppgifter om personer för att försöka värva dem som medlemmar. Här är det viktigt att komma ihåg att en registrerad har rätt att invända mot att föreningen fortsätter behandla hens uppgifter med intresseavvägningen som stöd.

Exakt hur en intresseavvägning ska vara formulerad är svårt att ge en mall för. Mycket är beroende av vilken grupp av personer det är fråga om, vilket ändamål det gäller och vilka typer av uppgifter som är aktuella att behandla.

I den ena vågskålen lägger vi vilka berättigade intressen organisationen anser sig ha, till exempel att kunna sprida information om sin verksamhet. I den andra vågskålen lägger vi i vilken omfattning och på vilka sätt den aktuella behandlingen skulle kunna innebära intrång i personlig integritet.

Relevant underlag vid en intresseavvägning är också vilka åtgärder organisationen kommer att vidta för att behandla uppgifterna korrekt och säkert, att bara använda dem på ett sjyst sätt, att inte sprida uppgifter vidare till andra för andra ändamål och så vidare.

Intresseavvägningen behöver vi naturligtvis bara göra en gång per typ av behandling. Inte för varje enskilt behandlingstillfälle av samma typ.

Vad gäller samtycke är rekommendationen att undvika beroende av det så långt det är möjligt. Om samtycke blir aktuellt är det viktigt att den som samtycker får klar och tydlig information om vad samtycket avser och att samtycket går att återkalla när som helst.

Ett samtycke ska vara en otvetydig viljeyttring men behöver inte alla gånger vara skriftligt. Den personuppgiftsansvariga – som har bevisbördan – måste dock ha ett sätt att styrka hur samtycke har blivit lämnat. Är det inte i form av skriftligt samtycke från varje berörd person kan det vara i form av skriftlig dokumentation av hur rutinen ser ut för att inhämta samtycken på annat sätt.

Oavsett vilken rättslig grund som blir aktuell för att ge stöd åt en viss behandling av personuppgifter för ett visst ändamål är det viktigt att tänka på att den grunden enbart ger stöd åt behandlingen så länge ändamålet är oförändrat. Sker en förändring, då är det fråga om en ny behandling. Som kan ha en helt annan rättslig grund. Men vänta ett tag, nu har vi använt orden ”behandla” och ”behandling” närmare fyrtio gånger, utan att förklara närmare vad de betyder i detta sammanhang. För att kunna dokumentera behandlingar av personuppgifter är det naturligtvis nödvändigt att ha klart för sig vad begreppet behandling står för.

Behandling av personuppgifter är varje åtgärd eller kombination av åtgärder som rör personuppgifter. Allt från insamling, registrering och organisering till begränsning, radering och förstöring. Med en mängd möjliga åtgärder som till exempel lagring, läsning, ändring, bearbetning och sammanföring däremellan.
Vad som utgör en avgränsad behandling är ibland inte helt lätt att avgöra. Beskrivningarna kan lätt bli både för detaljerade och för generella.

Några nyckelegenskaper är ändamålet, den rättsliga grunden, gruppen av berörda personer och de typer av uppgifter som är aktuella. Bildar dessa en sammanhållen logisk enhet, då är det med stor sannolikhet en (1) behandling. Förekommer två eller flera ändamål, två eller flera rättsliga grunder, två eller flera grupper av personer och så vidare, då är det lämpligt att beskriva det som sker som flera separata behandlingar.

4. Översyn av leverantörer och kontakter

Personuppgiftsbiträden är de leverantörer av tjänster den ansvariga tar hjälp av för att behandla personuppgifter. Det kan till exempel vara en extern förvaltare som hanterar bokföring eller ett tryckeri som hanterar adressuppgifter för att ordna med ett utskick till medlemmar. Den ansvariga bestämmer fortfarande ändamål och medel för behandlingarna, och ska ha reglerat detta i avtal med sina biträden.

En viktig del i ett biträdesavtal är att biträdet endast får behandla personuppgifter enligt dokumenterade instruktioner från den ansvariga. Biträdet ska ge garantier för korrekthet och säkerhet i samband med uppdraget att behandla uppgifter för den ansvarigas räkning. Biträdet kan i sin tur anlita ett biträde (en underleverantör), men får inte göra det utan att först inhämta tillstånd från den ansvariga. Avtalet bör också reglera vad som ska ske med uppgifterna när avtalet med biträdet löper ut.

En speciell situation är när biträdet är en stor aktör, till exempel en leverantör av molntjänster. Då är det oftast inte möjligt att upprätta ett regelrätt biträdesavtal. Den ansvariga får istället granska företagets allmänna villkor och integritetspolicy för att säkerställa att dessa standardformuleringar stämmer överens med de villkor som ett biträdesavtal annars skulle ha innehållit.

Andra externa tredje parter den ansvariga lämnar ut personuppgifter till kan också förekomma. Ett exempel är myndigheter som får kontrolluppgifter från organisationen. Dessa tredje parter behandlar uppgifterna för egna ändamål, på eget ansvar. Den ansvariga ska dock ha försäkrat sig om att den mottagande parten har dokumenterade skyddsåtgärder. Dessa externa tredje parter är således inte biträden den ansvariga tar hjälp av för sina egna behandlingar av uppgifter utan just externa tredje parter uppgifter blir utlämnade till.

5. Uppgiftshantering

Personuppgiftsansvarig ska säkerställa att personuppgifterna som behandlas är riktiga och korrekta d v s att de uppdateras (rättas eller raderas) på ett systematiskt och kontinuerligt sätt. Samt att det finns dokumentation kring tidsfrister och rutiner för lagring av personuppgifter d v s hur länge organisationen sparar uppgifterna i register/system. I de fall det inte går att uppge en exakt lagringstid ska tiden för lagring anges på ett sådant sätt att givaren kan göra en uppskattning av lagringstiden. Uppgifterna får i inget fall sparas under en längre tid än vad som är nödvändigt för ändamålen. När uppgifterna inte längre behövs för de ändamålen ska de raderas eller avidentifieras. Personuppgifterna kan sparas längre endast om det finns arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål samt lämpliga skyddsåtgärder för de registrerades rättigheter. Tidsfrister och rutiner för lagring ska dokumenteras.

Ur ett kartläggningsperspektiv kan det också vara ett bra angreppssätt att spalta upp organisationens behandlingar både utgående från grupper av registrerade personer och utgående från systemen som förekommer. Som ett sätt att säkerställa att ingen behandling har förblivit oupptäckt.

Med system menar vi här den vidare betydelsen som omfattar både manuella och automatiska processer. Hur våra arbetsordningar och rutiner ser ut och fungerar är minst lika viktigt som hur våra IT-system är utformade.

Ofta är det också genom att förändra eller bättre dokumentera de manuella rutinerna som det går att nå störst förbättringseffekt på kortast tid.

Den som svarar för behandlingen av uppgifter i ett system svarar inte bara för de manuella rutinerna utan också för att tekniska åtgärder är vidtagna. Även om det är någon annan som tillhandahåller systemet. Här ligger det nära till hands att jämföra med beställarens ansvar för att ställa rätt krav vid upphandling.

Några exempel på tekniska åtgärder som kan vara lämpliga för att uppnå bättre säkerhet är behörighetskontroller, kryptering av data och loggning av händelser i ett system. Tekniska åtgärder är dock inte mycket värda om de inte samtidigt är ackompanjerade av organisatoriska åtgärder för att skapa förståelse för varför de tekniska begränsningarna och kontrollerna existerar.

En inte helt ovanlig upptäckt vid kartläggning av system är att det förekommer personuppgiftsbiträden vi inte uppmärksammat tidigare. Om vi till exempel har en leverantör som står för driften av en server, då är det företaget vårt biträde. Även om deras personal inte hanterar uppgifterna direkt så svarar de för att lagra dem.

6. Individens rättigheter

De registrerade personerna har rätt till klar och tydlig information om vilka uppgifter om dem som vi behandlar.

Ett absolut minimum att informera om är den personuppgiftsansvarigas identitet, ändamålen med behandlingen, den rättsliga grunden och hur länge behandlingen kommer att fortgå, samt eventuella tredje parter uppgifter kan bli utlämnade till. Om uppgifterna inte är insamlade från de registrerade själva ska de även få information om från vilka källor uppgifterna kommer.

Vidare ska de registrerade få information om hur de kan ta till vara sina rättigheter när det gäller att begära tillgång till uppgifter, att begära rättelse eller radering av uppgifter och att lämna in klagomål till tillsynsmyndigheten Datainspektionen.

Förutom att det är en rättighet för de registrerade ligger det också i organisationens eget intresse att uppgifterna är kompletta och korrekta. Inte minst därför ska kontaktuppgifter till den som behandlar uppgifter alltid ingå i informationen som blir lämnad till de registrerade.

Informationstexter kan se olika ut för olika behandlingar och olika grupper av registrerade.

Vid insamling av uppgifter och vid övrig kommunikation med de registrerade går att ge en kortare version av information, så länge den innehåller en hänvisning till en längre version. En praktisk lösning i till exempel webbformulär eller e-postmeddelanden är att länka vidare till fördjupad information på en separat webbsida. I ett webbformulär kan ibland vara lämpligt att ha en kryssruta där den registrerade bekräftar att informationen har blivit lämnad (”Jag har tagit del av informationen om hur XXX behandlar mina uppgifter”). Observera att detta inte är samma sak som att den registrerade godkänner eller lämnar sitt medgivande. I de sällsynta fall den ansvariga behöver inhämta samtycke ska det vara en fråga som är klart och tydligt skild från andra frågor.

Från den information som avser en specifik behandling av uppgifter kan också vara lämpligt att länka till en webbsida med generell information om hur organisationen hanterar personuppgifter. På en sådan sida kan också organisationens integritetspolicy vara publicerad.

<u>Registerutdrag</u>

En registrerad person har enligt förordningen rätt att begära registerutdrag, på enkelt sätt och med rimliga intervall. Praxis för ”rimliga intervall” är en gång per år. Den registrerade ska få registerutdraget inom en månad från det att begäran inkom.

Även om troligen väldigt få personer kommer att vilja nyttja denna rätt måste vi vara förberedda på att ta fram utdrag som visar vilka uppgifter vi behandlar om en person. När vi ska leta fram dessa uppgifter är det naturligtvis vårt behandlingsregister vi använder som karta att orientera oss efter.

7. **Säkerhet**

Den ansvariga ska vidta både tekniska och organisatoriska åtgärder för att säkerställa en god säkerhet. Trots det kan incidenter inträffa. Vid en personuppgiftsincident ska den ansvariga inom högst 72 timmar anmäla det till tillsynsmyndigheten Datainspektionen. Vid en allvarlig incident ska även de registrerade personerna få information om det inträffade. Därför måste vi på förhand veta hur vi ska agera om olyckan är framme.

Några exempel på sådant som kan brista är följande.

- Har vi oklarheter kring ansvarsförhållandena?
- Ägnar vi oss åt ändamålsglidning (att vi fortsätter behandla gamla uppgifter för nya ändamål)?
- Har vi osäkerhet kring de rättsliga grunderna?
- Behandlar vi irrelevanta uppgifter?
- Sparar vi uppgifter alldeles för länge? Saknar vi gallringsregler?
- Har vi brister i säkerhet? Avser det i så fall tekniska eller organisatoriska åtgärder?
- Är vi dåliga på öppenhet gentemot de registrerade?
- Saknar vi rutiner för registerutdrag eller rättelser?

För att avgöra vilka åtgärder som ska ha högst prioritet måste vi göra en bedömning av risker och konsekvenser förknippade med respektive identifierat gap mellan teori och praktik. Vad skulle en viss brist kunna ha för negativa följder? Hur många skulle vara berörda av det? Vad är det värsta som skulle kunna hända och hur stor är sannolikheten för att det ska inträffa?

Är det inget som är undantaget från förordningen?

Tidigare under Personuppgiftslagen (PUL) var uppgifter i ostrukturerat material undantagna från hanteringsreglerna, enligt den så kallade missbruksregeln i §5a i PUL. Dataskyddsförordningen har inget sådant undantag.

Det enda lilla undantag som går att finna i förordningen är det som gäller för behandlingar som företas på annan väg än automatisk och där uppgifterna inte kommer att ingå i ett register. I praktiken betyder det:

Uppgifter vi har på papper och enbart på papper, och vi aldrig kommer att föra över i någon form av elektronisk lagring (inte ens fotografera eller skanna dem).

En rimlig utgångspunkt är därför att förordningens regler gäller för nästan allt ostrukturerat material. Vi måste därför i högre utsträckning än tidigare under PUL dokumentera hur vi behandlar personuppgifter i ordbehandlingsprogram, publiceringsverktyg, kalkylprogram och e-postprogram, samt i bild- och ljudupptagningar. Många har frågat sig: Hur ska det gå till?

När vi kartlägger behandlingar av uppgifter i ostrukturerat material gör vi precis som med andra behandlingar. Vi beskriver vilka grupper av personer som är berörda, vilka ändamål och rättsliga grunder vi har, vilka typer av uppgifter vi behandlar och så vidare. Inledningsvis på en övergripande nivå, för att vid behov förtydliga beskrivningarna på detaljnivå allt eftersom.

Många behandlingar kommer av naturliga skäl att bli mycket generellt beskrivna, på nivån att de registrerade tillhör kategorin *människa* och att de typer av uppgifter som kan förekomma är *löpande text* och *bild*. Viktigare blir då rutinerna för en korrekt och säker hantering och att bara behandla de uppgifter som är nödvändiga för det aktuella ändamålet. Att vi har en tillräcklig skyddsnivå för uppgifterna. Att vi inte behandlar irrelevanta uppgifter eller gör det på ett sätt som kan vara kränkande. Att vi gallrar de uppgifter vi inte längre behöver.

För de flesta är allt detta tämligen självklart. Till exempel samlar vi endast kontaktuppgifter till dem vi har ett berättigat intresse att kontakta och vi samlar just kontaktuppgifter och inte andra känsliga uppgifter. Likväl ska vi ha dokumenterat att det är dessa självklara principer vi följer.

Att över huvud taget ha börjat kartlägga behandlingar av uppgifter i ostrukturerat material är så mycket bättre än att ha blundat för det helt och hållet. Vi ska också ha i minnet att det slopade undantaget för ostrukturerat material är relativt nytt och ännu inte har blivit prövat i praktiken. Förhoppningen är att tillsynsmyndigheten Datainspektionen snart ska publicera en vägledning på detta område.

De delar av en verksamhet som har journalistiska ändamål är däremot undantagna från många av Dataskyddsförordningens regler. Här gäller istället Tryckfrihetsförordningens regler. Detsamma gäller för akademiskt, konstnärligt eller litterärt skapande.

Det som ligger inom ramen för journalistiska ändamål är att informera, utöva kritik och väcka debatt om samhällsfrågor. Även till exempel en blogg *kan* ha journalistiska ändamål. Att en organisation informerar om sin egen verksamhet är däremot inte journalistik i ordets rätta betydelse. Det går inte att vara en självständig bevakare av sig själv.

Viktigt att komma ihåg är att undantaget för journalistiska ändamål inte är avsett att fungera som ett kryphål för att slippa undan Dataskyddsförordningens regler. Slippa undan är dessutom fel ord, eftersom det istället blir fråga om att efterleva Tryckfrihetsförordningens regler.

Vill du läsa mer så finns följande länkar:
https://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/

MALLTEXT FÖR REGISTERUTDRAG

Hej,
Du har begärt att få ett s.k. registerutdrag från oss.

De personuppgifter som vi behandlar rörande dig, samlade vi in i syfte att kunna hantera ditt [fyll i ert syfte med att samla in uppgifterna här]. Vidare kan vi spara uppgifter rörande dig för lagkrav såsom bokföringslagen. Uppgifterna sparar vi så länge du är medlem(givare) och därefter i 36 månader i marknadsföringssyfte, samt för den tid som det finns lagstadgat att vi ska spara uppgifterna, exempelvis bokföringslagen är det 7 år.

De personuppgifter vi har samlat in är; ditt namn och adress, e-postadress, mobiltelefonnummer [kompletterat med de uppgifter ni har samlat in]. Du kommer även att få ta del av de noteringar som vår personal har gjort om dig om du har varit i kontakt med oss. För vissa behandlingar har vi tagit hjälp av underleverantörer (biträden). Vi har biträdesavtal med dessa för att säkerställa en korrekt hantering.

Som grund för behandling av dina personuppgifter har vi använt oss av medlemsvillkoren och berättigat intresse [fyll i syfte efter behov]. Om du vill ändra/rätta/radera/begränsa eller på annat sätt invända mot eller har frågor om vår behandling av dina personuppgifter kan du kontakta oss på adress: [e-postadress] av. Skulle du anse att vi inte behandlar dina uppgifter på ett korrekt sätt kan du även kontakta datainspektionen på datainspektionen@datainspektionen.se

Med vänlig hälsning
XX

EXEMPELMALL FÖR BITRÄDESAVTAL

(ska ej användas rakt av utan anpassningar till det enskilda fallet)

1. PARTER

Mellan Organisationen (org. nr. XXXXXXXX), Adress nedan ”Personuppgiftsansvarig”
och [Underleverantör Företaget AB] [org.nr.], [adress] nedan ”Personuppgiftsbiträde”
ingås härmed personuppgiftsbiträdessavtal enligt nedan.

2. SYFTE

Syftet med detta personuppgiftsbiträdesavtal är att tillse att Personuppgiftsbiträdets behandling av personuppgifter inom ramen för utförandet av [#] för den Personuppgiftsansvariges räkning, enbart sker i enlighet med den Personuppgiftsansvariges instruktioner, i överensstämmelse med detta biträdesavtal och i övrigt enligt de krav som framgår av 30 § personuppgiftslagen (1998:204) samt, vid dess ikraftträdande, artikel 28 i Dataskyddsförordningen (Europaparlamentets och Rådets Förordning (EU) 2016/679).

3. DEFINITIONER

Detta biträdesavtal ska tolkas i enlighet med – och ha de definitioner som framgår av – 3 § personuppgiftslagen eller, vid dess ikraftträdande, artikel 4 Dataskyddsförordningen.

4. PERSONUPPGIFTSANSVARIG

Personuppgiftsansvarig är skyldig att efterleva personuppgiftslagen samt, vid dess ikraftträdande, Dataskyddsförordningen, avseende personuppgiftsbehandling och anlitande av biträde. Personuppgiftsansvarig har rätt att styra Personuppgiftsbiträdets personuppgiftsbehandling och ska härvid meddela de dokumenterade instruktioner som behövs för Personuppgiftsbiträdets behandling.

5. PERSONUPPGIFTSBITRÄDETS ANSVAR

Personuppgiftsbiträdet ska endast behandla personuppgifter i enlighet med dokumenterade instruktioner.

6. SÄKERHETSÅTGÄRDER

Personuppgiftsbiträdet ska vidta och upprätthålla lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna, utan att ha rätt till särskild ersättning för detta. Personuppgiftsbiträdets säkerhetsåtgärder ska åstadkomma den skyddsnivå som följer av tillämplig lag samt, vid dess ikraftträdande, Dataskyddsförordningen och som i övrigt är lämplig med beaktande av tekniska möjligheter, kostnad för genomförande, särskilda risker med behandlingen och i vilken utsträckning de behandlade personuppgifterna är, eller sannolikt kan uppfattas som, känsliga. Personuppgiftsbiträdet ansvarar för att den egna verksamheten bedrivs på ett sätt som i övrigt säkerställer adekvat informationssäkerhet.

7. INCIDENTER

Personuppgiftsbiträdet ska vid konstaterad eller misstänkt säkerhetsincident, såsom obehörig åtkomst, förstörelse, ändring eller annan otillåten påverkan avseende personuppgifterna omedelbart undersöka incidenten, vidta lämpliga åtgärder för att åtgärda densamma och för att förhindra upprepning samt informera den Personuppgiftsansvarige genom att tillhandahålla Incidentrapport.

8. ÖVERFÖRING TILL TREDJE PART

Personuppgiftsbiträdet får inte överföra personuppgifter till tredje man och får heller inte lämna ut information om personuppgiftsbehandlingen till tredje man, utan att i förväg inhämta skriftligt godkännande av den Personuppgiftsansvarige.

9*. UNDERLEVERANTÖRER (UNDERBITRÄDEN)*
För anlitande eller ersättande av underleverantör för utförande av uppgift som innefattar personuppgiftsbehandling (Underbiträde), ska Personuppgiftsbiträdet först begära skriftligt godkännande för undertecknande av behörig företrädare hos den Personuppgiftsansvarige. Sådan begäran ska innehålla uppgift om Underbiträdets bolagsnamn och kontaktuppgifter, tjänstetyp, säte och geografisk placering av infrastruktur relevant för behandlingen av personuppgifter, samt andra uppgifter om Underbiträdet som begärts av den Personuppgiftsansvarige. Personuppgiftsansvarig har rätt att med bindande verkan motsätta sig anlitandet av visst Underbiträde om rimligt fog därför finns.

10. INSYN
I syfte att säkerställa upprätthållandet av lämplig säkerhetsnivå och efterlevnad av detta biträdesavtal, har Personuppgiftsansvarig rätt till erforderlig insyn i de delar av Personuppgiftsbiträdets organisation och system som relaterar till personuppgiftsbehandlingen. Vid behov ska biträdet vid ge tillsynsmyndigheten insyn.

11. SÄRSKILD ERSÄTTNING
Personuppgiftsbiträdet har inte rätt till särskild ersättning för fullgörandet av ansvar och skyldigheter enligt detta biträdesavtal eller för att följa de instruktioner avseende personuppgiftsbehandling som meddelas av den Personuppgiftsansvarige, annat än då det framgår av skriftlig överenskommelse.

12. ANSVAR FÖR SKADA
Om Personuppgiftsbiträdets behandling av personuppgifter eller underlåtenhet därvid, i strid med detta biträdesavtal eller med instruktion från Personuppgiftsansvarig, åsamkar Personuppgiftsansvarig skada, ska sådan skada ersättas av Personuppgiftsbiträdet.

13. ÖVERLÅTELSE AV AVTALET
Överlåtelse av detta biträdesavtal får endast ske i samband med överlåtelse av Huvudavtalet och då i enlighet med detsamma.

14. AVTALSTID
Detta avtal gäller från datum för underskrift och så länge Personuppgiftsbiträdet lagrar eller på annat sätt vidtar personuppgiftsbehandling för den Personuppgiftsansvariges räkning. Vid biträdesavtalets upphörande ska Personuppgiftsbiträdet enligt den Personuppgiftsansvariges instruktion radera eller återlämna all data innehållandes personuppgifter, på samtliga media varpå personuppgifter fixerats, samt därefter radera eventuella kopior.

15. TVISTER OCH TILLÄMPLIG LAG
Svensk rätt tillämpas på avtalet. Efter Tvist i anledning av detta biträdesavtal ska avgöras i enlighet med Huvudavtalets bestämmelse avseende tvistlösning.

16. ÄNDRINGAR
Ändringar och tillägg i detta biträdesavtal ska för giltighet upprättas skriftligen och undertecknas av båda parterna

Detta biträdesavtal har upprättats i två likalydande exemplar varav parterna har tagit var sitt och utgör vid undertecknande del av Huvudavtal såsom tilläggsavtal

Ort och datum	Ort och datum
Namnteckning	Namnteckning
Namnförtydligande	Namnförtydligande
Behörig firmatecknare	Behörig firmatecknare

Namnteckning

Namnförtydligande
Behörig firmatecknare