Vägledning vid upprättande av registerförteckningar SKK

1 Personuppgiftsansvarig – definieras i artikel 4

Personuppgiftsansvarig

Personuppgiftsansvarig är den som behandlar personuppgifter i sin verksamhet, det vill säga ofta ett företag, en myndighet eller en organisation. I ditt fall förmodligen din klubb.

Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter. (3 § personuppgiftslagen, artikel 4 förordningen.)

Personuppgiftsansvarig är normalt den juridiska person (till exempel aktiebolag, stiftelse eller förening) eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad de ska användas till. Det är alltså är inte VD, anställd eller **medlemsansvarig, kassör** i en klubb som är personuppgiftsansvarig, utan **klubben**, företaget eller föreningen**.** Undantagsvis kan en fysisk person vara personuppgiftsansvarig, till exempel en enskild företagare.

Det är de faktiska omständigheterna i det enskilda fallet som avgör vem som är personuppgifts-ansvarig. Avtal där ansvaret preciseras kan ge vägledning vid bedömningen. Om två eller flera gemensamt bestämmer över en viss behandling är de personuppgiftsansvariga tillsammans.

En användare som enbart har rätt att komma åt personuppgifter genom att läsa dem och söka bland dem men som inte självständigt får ändra, komplettera eller radera uppgifterna är **inte** person-uppgiftsansvarig.

1.1

Döp varje register. Försök benämn registret så att alla som läser namnet förstår vilket register som avses.

1.2

Informationsägare är den som ytterst ansvarar för registret (för den personuppgiftsansvariges räkning). Det är vanligen en person i klubben, kanske sekreteraren, kassören eller den tävlingsansvarige.

Är det exempelvis en förteckning över en kurs bör kurskansliets administratör anges som informationsägare. Informationsägaren ska vara den person som är den som vanligen handskas med registret. Om flera handskas med registret får dessa tillsammans utse vem som ska vara registrets informationsägare.

2 Registret/Personuppgiftsbehandlingen

Uppgifterna avser:

Fyll i om behandlingen avser ny behandling eller enbart innehåller ändringar eller om registret raderas/makuleras. Även om registret raderas kan det vara bra att behålla uppgifter om registret utifall att Datainspektionen ställer en fråga eller om den som behandlingen avser inkommer med en begäran om registerutdrag. Det kan då vara bra att känna till att registret har funnits men numera inte finns.

2.1

För att enkelt kunna besvara en förfrågan eller en begäran kan det vara bra att känna till var behandlingen sker och var den lagras. Kunskap om detta behövs även för att på bästa sätt kunna radera uppgifter, rätta uppgifter samt se till att adekvat skydd för uppgifterna finns.

3 Personuppgifterna

Ange om någon av nedanstående kategorier av personuppgifter behandlas:

Fyll noggrant i vilka uppgifter som behandlas. För varje behandling gäller att uppgifterna samlas in för särskilt uttryckliga och berättigade ändamål. De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (*uppgiftsminimering, artikel 5 förordningen*).

4 Ändamålet – artikel 5

Uppge ändamålet/ändamålen med personuppgiftsbehandlingen. Det ska tydligt, detaljerat och specifikt framgå vad uppgifterna faktiskt ska användas till och vad som är syftet/ändamålet med att de behandlas.

Här skrivs essensen av ändamålet med behandlingen. Om registret exempelvis rör en kurs, skriver klubben att ändamålet med behandlingen är att få information om kursdeltagarna för att kunna göra utskick med information om kursen, dess delmoment, start- och slutdatum etc. Om all kommunikation sker via mejl behöver inte uppgifter om adress behandlas och de ska då inte finnas med i registret. Om registret i stället rör ett medlemskap skriver man att ändamålet med behandlingen är att kunna administrera den registrerades medlemskap, utskick och information, inbjudningar etc.

5 Laglig behandling av personuppgifter – artikel 6

Behandling är endast laglig om och i den mån som åtminstone ett av följande villkor är uppfyllt:

För att behandlingen ska vara laglig krävs att någon av de fem uppställda grunderna är uppfyllda. (Det finns ytterligare två lagliga grunder i artikel 6 men då SKK inte kan se att dessa är tillämpliga för klubbarna har vi valt att utelämna dem som alternativ. Det rör bland annat myndighetsutövning och att skydda intressen av grundläggande betydelse för den registrerade.)

Eftersom ett samtycke kan återkallas och en intresseavvägning kan utfalla till den registrerades fördel är det bra att grunda behandlingen på ett avtal, exempelvis ett avtal om medlemskap, kurs etc.

Exempel på personuppgiftsbehandling som kan vara nödvändig i samband med avtal är kundsystem för bland annat fakturering.

Om anmälan till kurs eller medlemskap går att göra via hemsidan bör klubben införa en ruta där den registrerade måste intyga att denne har tagit del av ändamålen med behandlingen och att det krävs för att bli medlem, gå kurs etc. Det ska då tydligt framgå att det rör sig om ett avtalsförhållande, om så är fallet, eller att den registrerade samtycker till behandlingen, dvs det ska finnas ett giltigt dokumenterat samtycke/avtal som klubben kan visa upp, exempelvis en logg, en underskrift osv.

En behandling som grundar sig på rättslig förpliktelse kan exempelvis vara att klubben sparar sina fakturor (som ofta innehåller personuppgifter) då klubben enligt lag har en skyldighet att spara sin bokföring i sju års tid.

En behandling som grundar sig på ett allmänt intresse kan vara arkivering och forskning.

När det gäller berättigat intresse kan det vara i klubbens intresse att behandla personuppgifter om en utesluten medlem eller en medlem som valt att avsluta sitt medlemskap i samband men en disciplinär prövning. Då väger klubbens intresse av att ha kvar kunskapen om medlemmen och att denne inte får bli medlem igen utan prövning av Disciplinnämnden högre än medlemmens intresse av att exempelvis bli glömd/raderad.

6	**Den registrerades rätt till tillgång – artikel 15** *Enligt artikeln har den registrerade rätt att få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till dessa. Den personuppgiftsansvarige ska förse den registrerade men en kopia av de personuppgifter som är under behandling.*

Rätt till tillgång

Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen 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) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

Informationen ska tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form (vilket kan vara i elektronisk form) och med ett tydligt och enkelt språk. I dataskyddsförordningen anges utförligt vilken information som ska ges. Bland annat ska information lämnas om kontaktuppgifter till den personuppgiftsansvarige, den rättsliga grunden för behandlingen och ändamålet med behandlingen.

7	**Säkerhet i samband med behandlingen – artikel 32** *Vilka åtgärder har vidtagits för att trygga säkerheten i behandlingen:*

Säkerhet enligt personuppgiftslagen/dataskyddsförordningen

Hur man bedömer lämpliga säkerhetsåtgärder

För alla som hanterar och bearbetar personuppgifter är det viktigt att säkerställa att person-uppgifterna skyddas på ett bra sätt. Enligt personuppgiftslagen, såväl som dataskyddsförordningen,

ska den som är personuppgiftsansvarig vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna. Till tekniska åtgärder räknas saker som brandväggar, krypterings-funktioner och anti-virus, medan organisatoriska åtgärder handlar om säkerhetsarbetets organisation och rutiner, instruktioner och policys.

Generellt gäller att ju känsligare personuppgifterna är eller ju fler personuppgifter som hanteras, desto mer omfattande bör säkerhetsåtgärderna vara.

När man gör en lämplighetsbedömning, det vill säga bestämmer vilken säkerhetsnivå man ska ha, ska man tänka på att åtgärderna ska ge en säkerhetsnivå som är lämplig i förhållande till:

- tillgänglig teknik
- kostnaden för åtgärderna
- om det finns några särskilda risker med behandlingen
- hur pass känsliga uppgifterna är

Med tillgänglig teknik menas de tekniska lösningar som i dagsläget är tillgängliga på marknaden. Det kan också ses som en referens till att i första hand använda produkter som stödjer etablerade, välbeprövade standarder.

Kostnaden för säkerhetsåtgärderna ska ställas i relation till riskerna för att obehöriga får ta del av personuppgifterna. Ju större riskerna är, desto mer omfattande ska säkerhetsåtgärderna vara.

Den som är personuppgiftsansvarig ska ta ställning till vilka särskilda risker det finns med behandlingen. Finns det sådana risker kan det påverka vilka säkerhetsåtgärder som behövs för att skydda personuppgifterna. Frågor man bör ställa sig är:

- Behandlas personuppgifterna på ett sätt som gör det svårt att kontrollera att det bara sker i enlighet med ändamålen med behandlingen? Finns det risk för att personuppgifterna kan spridas på ett oönskat sätt?
- Hanteras personuppgifter via öppna nät som internet, till exempel via en webbhemsida eller genom e-post?
- Kan många användare komma åt personuppgifterna?
- Behandlas personuppgifter om många personer?
- Behandlas en stor mängd personuppgifter om varje person?
- Hur stor är sannolikheten för och konsekvenserna av tekniska störningar eller att obehöriga får åtkomst till uppgifterna?

Ju fler av dessa frågor som man svarar Ja på desto mer omfattande bör säkerhetsåtgärderna vara.

Enligt personuppgiftslagen, såväl som dataskyddsförordningen, gäller särskilda begränsningar för behandling av vissa kategorier av personuppgifter. I lagen betecknas dessa uppgifter som "känsliga" personuppgifter. Känsliga personuppgifter är enligt personuppgiftslagen sådana som avslöjar: ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, uppgifter som rör hälsa eller sexualliv och det är därför inte aktuellt för SKKs medlemsorganisationer.

Personuppgifter som normalt sett inte är integritetskänsliga i lagens mening är uppgifter som rör exempelvis anställningsförhållanden, kundförhållanden och medlemsregister. Normalt sett harmlösa personuppgifter kan dock bli känsliga beroende på i vilket sammanhang de förekommer.

8 Gallring

Hur länge får man bevara personuppgifter?

Ett grundläggande krav i personuppgiftslagen, såväl som i dataskyddsförordningen, är att personuppgifter inte ska bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Sedan är det dock så att personuppgifter får bevaras för historiska, statistiska eller vetenskapliga ändamål under längre tid än som anges ovan. Uppgifterna får dock inte bevaras längre än vad som behövs för dessa ändamål.

Hur vet man när man ska ta bort personuppgifter?

Kortfattat kan man säga att det är ändamålet, det vill säga anledningen till att personuppgifterna behandlas, som avgör hur länge uppgifterna får bevaras i identifierbart skick. Men hur ska den personuppgiftsansvarige i praktiken veta när personuppgifter inte längre får bevaras? Enligt personuppgiftslagen får den personuppgiftsansvarige samla in personuppgifter bara för särskilda, uttryckligt angivna och berättigade ändamål. Ändamålen måste bestämmas redan när uppgifterna samlas in och kunna anges uttryckligen. Helst bör ändamålen därför skrivas ned.

Uppgifterna får inte bevaras om de av någon anledning inte längre kan anses vara riktiga och relevanta, det vill säga blivit ovidkommande i förhållande till ändamålet. Finns det till exempel i en sporthandlares kundregister antecknat att en kund har golf som intresse, och uppgiften är relevant därför att sporthandlaren säljer golfartiklar och därför har ett intresse av att veta vilka kunder han ska rikta sina reklamerbjudanden mot, är uppgiften inte längre relevant om handlaren slutar att sälja just golfartiklar. Uppgiften bör då tas bort.

Uppgifter får alltså inte samlas in bara för att de eventuellt kan komma till användning vid ett senare tillfälle och därför kan vara bra att ha. Om en personuppgift av någon anledning blir överflödig får den inte längre bevaras.

Det räcker dock inte med att den personuppgiftsansvarige uttryckligen har angett ett särskilt och berättigat ändamål för att uppgifterna ska få behandlas (och därmed bevaras). Behandlingen måste dessutom vara tillåten. Fullgörande av avtal är exempel på tillåten behandling. Skulle någon av förutsättningarna som anges i dessa bestämmelser för att behandling av personuppgifter ska vara tillåten inte längre föreligga får uppgifterna inte längre bevaras, eftersom det då inte längre är fråga om en tillåten behandling.

Hur tar man bort personuppgifter?

Det finns två olika sätt att ta bort personuppgifter. Man kan antingen avidentifiera eller förstöra dem.

Avidentifiera

Att avidentifiera personuppgifterna innebär att man avlägsnar alla identifieringsmöjligheter så att de uppgifter som fortsättningsvis behandlas inte längre går att koppla samman med en fysisk person.

Krypterade personuppgifter är inte avidentifierade så länge någon kan göra uppgifterna läsbara och därmed identifiera personen.

Förstöra

Att förstöra personuppgifterna innebär att se till att de inte går att återskapa. Det är viktigt att känna till vad som krävs rent tekniskt för att uppgifterna verkligen ska förstöras. Det är till exempel inte tillräckligt att radera den fil som innehåller personuppgifterna. Det är nämligen inte säkert att ett sådant kommando verkligen raderar all information, filen kan exempelvis ligga kvar i datorns "papperskorg". I stället krävs säker omformatering av lagringsmediet eller total överskrivning så att personuppgifterna inte kan tolkas i efterhand. Det är dock inte heller säkert att vanlig formatering raderar alla uppgifter utan det kan krävas särskild utrustning eller specialprogramvaror. Hur långtgående tekniska åtgärder som bör vidtas är bland annat beroende av informationens känslighet.

Utskrifter

Hur gör man då om man skrivit ut personuppgifterna på papper? Måste man då förstöra papperet? Eftersom själva utskriften av personuppgifterna i sig är en behandling måste man fundera över om utskriften är tillåten enligt personuppgiftslagens/förordningens bestämmelser. Om man skriver ut uppgifterna i samband med att de inte längre behövs för det ändamål som de samlades in för och utskriften görs enbart för att de ändå ska bevaras är utskriften inte tillåten enligt personuppgiftslagen (dataskyddsförordningen). Om utskriften görs därför att uppgifterna kan behövas i pappersform för andra ändamål, till exempel för bokföringsändamål, är utskriften däremot tillåten.

Hur ska man se till att personuppgifter inte bevaras för länge?

Vilka rutiner ska då den personuppgiftsansvarige ha för att se till att personuppgifter inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet?

Det är lämpligt att man redan i samband med att behandlingen av personuppgifter påbörjas tar ställning till hur länge uppgifterna i normalfallet ska bevaras och när de ska tas bort, det vill säga avidentifieras eller förstöras. För att underlätta arbetet kan man upprätta en "gallringspolicy" där man anger vilka uppgifter som kommer att behandlas, för vilket ändamål man behandlar dem och när de ska tas bort. Vidare kan en sådan policy innehålla en beskrivning av vilka rutiner man ska ha för att avidentifiera eller för att på ett säkert sätt förstöra uppgifterna.

Har den personuppgiftsansvarige utsett ett personuppgiftsombud kan det vara lämpligt att ombudet tillsammans med den personuppgiftsansvarige ser till att en sådan policy upprättas.

Några praktiska exempel

Medlemmar i ideella föreningar

När en medlem i en förening avslutar sitt medlemskap bör uppgifterna i medlemsregistret tas bort. Inget hindrar att uppgifter om medlemmen får finnas kvar tills dess att denne exempelvis har betalat utestående medlemsavgifter och lämnat tillbaka lånad utrustning.

Dessutom får personuppgifter om tidigare medlemmar normalt bevaras under ett år för att föreningen ska kunna värva tillbaka den som tidigare har varit medlem. Grunden för detta ställningstagande är att en sådan behandling har stöd i en intresseavvägning. Men om den tidigare

medlemmen dessförinnan tackar nej till att återigen bli medlem ska dennes personuppgifter tas bort snarast möjligt.

Direktmarknadsföring

Om det finns ett kundförhållande mellan kunden och den personuppgiftsansvarige får den personuppgiftsansvarige skicka reklam till kunden, om nu inte kunden har motsatt sig det, detsamma gäller för en medlemsorganisation i förhållande till sina medlemmar.

I normala fall får personuppgifter om en tidigare kund/medlem användas för marknadsförings-ändamål under ett års tid efter det att kundförhållandet har upphört, det vill säga efter det att varan eller tjänsten är levererad och betald samt att eventuell garantitid har löpt ut. Om han eller hon dessförinnan begär att bli struken ur registret ska personuppgifterna dock tas bort snarast möjligt.

Om en marknadsförare samlar in uppgifter om personer som det inte finns någon kund- eller medlemsrelation till för att använda dem till marknadsföring bör uppgifterna tas bort snarast efter det att de använts. Eftersom adressuppgifter ofta ändras och därför inte kan betraktas som aktuella under någon längre period bör de inte bevaras längre än tre månader från det datum då de samlades in.

Vid sidan av personuppgiftslagen (dataskyddsförordningen) finns det även en branschöverens-kommelse med regler för användning av personuppgifter vid direktmarknadsföring (läs mer på www.swedma.se). Dessutom regleras användningen av e-post i reklamsyfte till konsumenter i marknadsföringslagen (2008:486).

9 Extern personuppgiftsbehandling

Utförs behandlingen av personuppgifterna av någon utanför organisationen, det vill säga av någon extern part? (Exempelvis samarbetsklubb, SKKs kansli, tryckeri etcetera.)

Här är det viktigt att reflektera och dokumentera om andra än den/de personuppgiftsansvariga behandlar personuppgifterna. Det ska därför anges vem eller vilka i så fall och det **ska** upprättas personuppgiftsbiträdesavtal med dessa parter. Det bör också anges vem som är ansvarig för kontakterna med de externa parterna, vanligen den som undertecknat biträdesavtalet, eller dennes efterträdare, eller annan särskild dedikerad person. SKK har tagit fram ett personuppgiftbiträdesavtal som klubbarna kan använda.

10 Utlämnande – artikel 14

Följande mottagare har eller kan komma att erhålla personuppgifter (t ex myndigheter, klubbar, tryckeri, samarbetspartners, kommersiella företag):

För att kunna följa upp att all behandling sker i enlighet med förordningen bör man som personuppgiftsansvarig fundera över om personuppgifterna kommer eller kan komma att överlämnas till utomstående. Om man som personuppgiftsansvarig har för avsikt att överlämna uppgifterna till tredje part ska den registrerade få vetskap om vilka mottagare som ska få ta del av personuppgifterna. Vid utlämnande till tredje part ska den registrerade få vetskap om utlämnandet allra senast när personuppgifterna lämnas ut för första gången (artikel 14, 3 b).

11 Inhämtande inom organisationen

Har uppgifterna inhämtats ifrån annat IT-system inom organisationen?

För kunskap om var behandlingen sker/har skett och att uppgifterna är aktuella är det av vikt att känna till om de hämtas någon annanstans än där de behandlas för tillfället och i så fall säkerställa att informationen är adekvat på samtliga ställen där behandling sker.

12	**Inhämtande utanför organisationen – artikel 14** *Uppge om uppgifterna har inhämtats ifrån externa parter, till exempel samarbetspartners, IT-leverantörer, SPAR, Bisnode eller liknande.*

Om personuppgifterna inte har erhållits från den registrerade, ska den personuppgiftsansvarige förse den registrerade med följande information: identitet och kontaktuppgifter för personuppgifts-ansvarige och i tillämpliga fall för dennes företrädare. Ändamålen med behandlingen och den rättsliga grunden, vilka personuppgifter som behandlingen avser, varifrån personuppgifterna hämtas.

13	**Information till registrerade** *Har de registrerade informerats om behandlingen av personuppgifter?*

Eftersom det är krav på att den registrerade ska ha fått information bör JA-rutan vara ikryssad. Klubben bör även säkerställa hur denne ska kunna bevisa att information har lämnats, det är därför lämpligt att informationen lämnas skriftligt till den registrerade.

14	**Övrigt** *Skriv här*

Bra med extra plats för uppgift eller kommentar av vikt för den specifika behandlingen. Det ska också framgå vem som är behörig företrädare för klubben. Glöm inte att ändra dessa uppgifter om personen ändras, såväl som dennes kontaktuppgifter och datum för ändringen.