

# Anpassning till DSF

20180525

## Innehållsförteckning

Sammanfattning.....	2
Allmänna råd.....	4
Vi har lagring i flertalet miljöer som är uppdelat regional och lokalt.....	4
Tillgång till personuppgifter.....	4
Personer har rätt att veta vilka som ser deras information och varför.....	4
Ändamålsbeskrivning.....	4
Person som inte vill vara registrerad.....	5
Uppgiftsminimering.....	5
Kryptering av kommunikation.....	5
Hantering av ekonomiadministration (digitalt).....	5
Hantering av ekonomiadministration (på papper).....	5
Hantering av personuppgifter HR.....	5
Övervakning av incidenter.....	6
Säkerhetsinställningar för användare.....	6
Hantering av särskilda kategorier.....	6
Hantering av utskrifter av personuppgifter på papper.....	6
Hantering av utskrifter av personuppgifter digitalt.....	6
Data Portabilitet.....	6
Rättelse av personuppgifter.....	7
Rättigheter gällande vad användarna ser.....	7
Gallring.....	7
Texter på material.....	7
Kommunikation.....	7
Överföring av data till externa intressenter.....	7
Databas i Episerver.....	7

## **Sammanfattning.**

PRO måste från och med den 25:e maj 2018 anpassa hanteringen av personuppgifter enligt den nya lagen DSF, Dataskyddsförordningen.

PRO har genomfört analys av vilka personuppgifter vi hanterar och vilken typ av uppgifter. Det har skett en genomgång av var och hur dessa uppgifter lagras och hanteras, båda digitalt och på papper. DSF anger även att hanteringen av så kallade ostrukturerade uppgifter ska ingå i dokumentationen, detta kommer att ske i steg två av anpassningen. Genomgång av

våra IT lösningar har gjorts, säkerhetsmässigt och vilka processer som finns och är anpassade för DSF. En GAP analys har genomförts.

Nedan specificeras råd på hur PROs föreningar, samorganisationer och distrikt bör anpassa verksamheten för att anpassas till de direktiv som finns i DSF.

## **Allmänna råd.**

### **Vi har lagring i flertalet miljöer som är uppdelat regional och lokalt.**

Varje distrikt, samorganisation och förening är ansvariga för de personuppgifter ni samlar in och lagrar i er förening. Varje distrikt, samorganisation samt förening är personuppgiftsansvarig och ska följa de stadgar, beslut och policys som fastställs av PROs kongress, representantskap samt riks styrelse. Personuppgifterna som finns i PROs system ansvarar riksorganisationen för. Detta finns beskrivet i PROs policydokument och på [www.datainspektionen.se](http://www.datainspektionen.se).

### **Tillgång till personuppgifter.**

DSF kräver att alla personer har rätt att få information om de uppgifter som finns registrerade i våra register. Utdrag ur Hjördis och andra enheter med information måste lämnas till personen inom 30 dagar.

Vid förfrågan från person tas uppgifterna fram manuellt. De uppgifter som finns i Hjördis är personnummer, namn, adress, medlemsnummer föreningstillhörighet, samorganisationstillhörighet, distriktstillhörighet, reskontra, uppdrag och ansvarsområde, kurs/konferensdeltagande. Varje fråga måste besvaras inom 30 dagar och det måste finnas rutiner upprättade för detta. Uppgifterna förs upp i ett dokument som sänds via post till personen i fråga. Alla bör spara sina dokument med personuppgifter i PROs gemensamma arbetsyta på internet, Microsoft E365 där ni kan upprätta sökningar som tar fram uppgifter som finns på enstaka personer, på så sätt får ni även godtagbar IT säkerhet för personuppgifter.

### **Personer har rätt att veta vilka som ser deras information och varför.**

DSF kräver att personer ska få veta vem och varför någon tittat på deras uppgifter om de begär det.

Från och med den 24 maj är det endast personliga inloggningar som gör det möjligt att logga in i Hjördis, det gör att det finns en förteckning över vem som kan läsa våra personuppgifter. För att få en personlig inloggning krävs att man innehar ett uppdrag eller ansvarområde som är registrerat i Hjördis. Det är oerhört viktigt att uppdatera Hjördis med uppdrag och ansvarområden så att ingen obehörig kan logga in.

### **Ändamålsbeskrivning.**

DSF anger att man beskriver orsaken, syftet och till vad personuppgifterna används. Det innebär att varje insamling av nya personuppgifter måste dokumenteras med beskrivning av vilka uppgifter som samlas in, syftet med registreringen, hur uppgifterna används samt hur länge de sparas. De bör om inte det finns särskilda skäl raderas inom 6 månader efter att det inte finns något behov av dem.

### **Person som inte vill vara registrerad.**

Om en person meddelar att den inte vill finnas i våra register är vi skyldiga att radera och glömma personuppgifterna. Konsekvensen blir då att medlemskapet upphör då vi inte kan hantera medlemskap manuellt.

### **Uppgiftsminimering.**

Man får inte samla mer uppgifter än nödvändigt. Ni måste dokumentera begränsning av insamling av uppgifter så ni inte samlar på er mer än nödvändigt för att fylla ändamålskraven.

### **Missbruksregeln finns inte i DSF.**

I den gamla personuppgiftslagen fanns en missbruksregel som innebar att personuppgifter som fanns i löpande text undantogs från PUL. Denna regel är borttagen i DSF vilket betyder att alla personuppgifter innefattas av DSF även i löpande text på till exempel webbsidor.

### **Kryptering av kommunikation.**

DSF kräver att digital kommunikation som innehåller personuppgifter ska vara krypterad. I vår tjänst för e-post installeras MS ATP, Kryptering, som är en funktion som scannar utgående mail och varnar för att det kan innehålla personuppgifter. Om så är fallet föreslår systemet att mailet blir krypterat och kan inte öppnas av någon annan än den angivna mottagaren, det är heller inte möjligt att vidarebefordra mailet. Ni bör inte maila uppgifter om personer i något annat system än PROs egna. **(denna funktion håller på att installeras, mer information kommer när detta är klart)**

### **Hantering av ekonomiadministration (digitalt)**

All hantering bör ske i PROs datorer, all information bör sparas i PROs servermiljö, aldrig i egna datorn. Vid arbete ska uppmärksamhet finnas på om personer finns i närheten och kan läsa skärmen då tar vi bort uppgifterna på skärmen. Skärmen bör även ha sekretessfilter för att försvåra för utomstående att se innehållet på skärmen.

### **Hantering av ekonomiadministration (på papper)**

Alla papper som innehåller personuppgifter får inte finnas framme i allmänna utrymmen mer än nödvändigt. I lunchrum, reception, brevfack eller andra offentliga lokaler som till exempel kurs/sammanträdeslokaler får sådana dokument inte ligga överhuvudtaget. De ska aldrig ligga i skrivaren, uppgifterna skrivs ut under uppsikt och tas genast därifrån. När de inte används ska de förvaras i låsta skåp alternativt makuleras.

### **Hantering av personuppgifter HR.**

Om ni har anställda registreras deras personuppgifter i personaladministrativa system. Behandlingen av personuppgifterna är nödvändig för att kunna fullgöra avtalsenliga förpliktelser mot anställda samt för att PRO ska kunna fullgöra sina skyldigheter enligt

arbetsrätten och skattelagstiftningen; detta utgör också PRO:s lagliga grunder för personuppgiftsbehandlingen. Detta ska personalen informeras om och helst skriva avtal.

### **Övervakning av incidenter.**

Vid händelse av en incident som intrång i era system av obehörig eller felaktiga utdrag eller hantering av uppgifter ska rapporteras till Datainspektionen senast 72 timmar efter upptäckt.

### **Säkerhetsinställningar för användare.**

Vi går igenom rättigheter och justerar rättigheter i systemen kontinuerligt så att ingen ska ha tillgång till mer uppgifter än nödvändigt. Detta bör även ske i de lokala program ni använder.

### **Hantering av särskilda kategorier.**

Om ni har register som innehåller särskilda kategorier, ras eller etniskt ursprung politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person krävs en högre säker och kryptering, dessutom ska man ha ett ordentlig hållbart skäl för att lagra sådana uppgifter. Detta bör undvikas.

### **Hantering av utskrifter av personuppgifter på papper.**

DSF talar om att personuppgifter får ses eller delges endast de personer som har rätt till det, gäller även hantering av uppgifter på papper. Alla papper som innehåller personuppgifter får inte ligga framme i allmänna utrymmen I lunchrum, reception, brevfack eller andra offentliga lokaler som till exempel kurs/sammanträdeslokaler får sådana dokument inte ligga överhuvudtaget. De ska aldrig ligga i skrivaren, uppgifterna skrivs ut under uppsikt och tas genast därifrån. När de inte används ska de förvaras i låsta skåp alternativt makuleras.

### **Hantering av utskrifter av personuppgifter digitalt.**

DSF talar om att personuppgifter får ses eller delges endast de personer som har rätt till det, gäller även hantering av uppgifter på skärm. All hantering ska ske i PROs datorer, all information ska sparas i PROs servermiljö, aldrig i egna datorn. Vid arbete ska uppmärksamhet finnas på om personer finns i närheten och kan läsa skärmen då tar vi bort uppgifterna på skärmen. Skärmen ska även ha sekretessfilter för att försvåra för utomstående kan se innehållet på skärmen.

### **Data Portabilitet.**

PRO är skyldiga att sända en persons uppgifter vidare till annan organisation om personen anger att medlemskapet ska upphöra i PRO och överföras till annan organisation. Vid förfrågan från person tas uppgifterna fram. Varje fråga måste besvaras inom 30 dagar.

### **Rättelse av personuppgifter.**

Om en medlem upptäcker att det är fel registrerade uppgifter ska det snarast rättas.

### **Rättigheter gällande vad användarna ser.**

Samtliga som loggar in i Hjärdis ser inte bara sina egna medlemmar, till exempel en förening ser alla medlemmar inom PRO, men de kan endast administrera och ändra på sina egna. Vår bedömning är att föreningarna har en fördel och hjälp av att se alla medlemmar, det kan vara vid medlemsrekrytering (ny föreningsmedlem), sökfunktioner för att finna medlemmar i närområdet för att bjuda in till olika evenemang, söka förtroendevalda i närheten för samarbete etc.

### **Gallring.**

Enligt DSF får personuppgifter sparas så länge vi har behov av dem, de ska sedan gallras.

Vissa uppgifter sparas i 7 år enligt bokföringslagen (reskontra), andra ska genast gallras när behov inte finns, enligt uppgiftsminimeringen.

Era texter som informerar om DSF måste innehålla information om detta, rekommenderar att vi anger 7 år och orsaken annars får vi klagomål på att uppgifter finns kvar mer än två år.

### **Texter på material.**

Alla era material där personuppgifter inhämtas måste ha en text som beskriver hur och varför vi hanteras personuppgifter.

### **Kommunikation.**

När t.ex. namninsamlingar ska genomföras måste en uppgiftsminimering upprättas samt en konsekvensanalys genomföras, observera om uppgifterna är av särskilda kategorier, t.ex. politiska åsikter. Text med samtycke måste finnas på webbformulär och pappersunderskrifter, efter genomförd kampanj måste uppgifterna gallras. Ostrukturerade uppgifter på webben, bilder, namn i löpande text, ljudupptagningar måste ha ett medgivande, muntliga medgivanden är acceptabla men måste dokumenteras.

### **Överföring av data till externa intressenter.**

PROs personuppgifter får inte lämnas vidare till tredje part om inte detta är överenskommet med riksorganisationen.

### **Databas i Episerver.**

Alla redaktörer i Episerver har tillgång till formulärhantering för insamling av data. All information sparas i en databas som innehåller väldigt mycket data som inte kan kontrolleras. Under en period kommer denna funktion stängas så att data kan raderas och policy för hur detta ska hanteras är upprättad.