



## **1 kap. PERSONUPPGIFTSPOLICY FÖR UPPDRAGSTAGARE**

Använd den här policyn som en guide för att hjälpa dig i ditt GDPR-arbete. Om du har några frågor eller funderingar, kontakta Styrelsen: Styrelsen@dtek.se. Den här policyn skapades 2018 och uppdaterades 2020 som ett led i arbetet med att göra sektionen, dess kommittéer och intresseföreningar kompatibla med GDPR och ska om allt fungerar som det är tänkt uppdateras löpande.

### **1.1 Om GDPR och ideellt engagemang**

Det är viktigt att det är lätt och roligt att engagera sig ideellt på datateknologsektionen, även när vi behöver hålla oss till gällande lagar och regler. Därför försöker vi hålla administrationen kring GDPR till ett minimum. Följande behöver dock utföras för att vi ska följa lagen:

### **1.2 Vid inval**

Den nyinvalde ska så snart som möjligt skriva på ett kontrakt för att bli personuppgifts- behandlare, vilket innebär att den får samla in och hantera personuppgifter för Datateknologsektionen.

### **1.3 Vid inaktivitet**

Om en person slutar vara aktiv i en kommitté eller intresseförening förlorar den åtkomst till kommitténs personuppgifter tills den blir aktiv igen, detta för att minimera antalet personer med tillgång till personuppgifter.

### **1.4 Tredje parts åtkomst**

När personuppgifter delas med parter som ej är personuppgiftsbehandlare på Datateknologsektionen är de att anse som tredje part. Det förekommer att personuppgifter delas med tredje parter i olika delar av sektionens verksamhet.

#### **1.4.1 Huvudregel**

En tredje part kan få åtkomst till personuppgifter om det föreligger särskilda skäl, förutsatt att detta godkänns av personuppgiftsansvarige i Styrelsen. Vid sådana omständigheter ska personen i fråga även underteckna ovan nämnda kontrakt.

#### **1.4.2 Undantag**

Undantag från 5.4.1 är då personuppgiftsbehandlare nyttjar tredje parts tjänster på internet. Då skall personuppgiftsbehandlaren försäkra att tjänsten har en personuppgiftspolicy som är enligt med GDPR och ej delar sektionens personuppgifter med annan tredje part som ej uppfyller huvud- eller undantagsregeln.

Vid samarrangemang bör en personuppgiftsansvarig utses i den sektionskommitté som arrangerar med en tredje part. Dess uppgift är att säkerställa att den arrangerade kommittén hanterar personuppgifter som sektionen anser som lämpligt för att undantaget skall kunna tillämpas.



## **1.5 Dokumentation**

Styrelsen ska upprätthålla en lista över alla personer med åtkomst till personuppgifter, samt i vilka sammanhang de kommer åt dessa personuppgifter. Exempel på sammanhang är "Phixare i D6".

## **1.6 Behandling av personuppgifter**

GDPR är hårdare kring lagring av personuppgifter än den tidigare personuppgiftslagen (PUL). Nedan följer praktiska riktlinjer för hur personuppgifter ska hanteras med nya lagstiftningen.

### **1.6.1 Grundprinciper**

GDPRs grundprinciper är att man som personuppgiftsansvarig:

- Måste ha stöd i dataskyddsförordningen för att få behandla personuppgifter.
- Bara får samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål.
- Inte ska behandla fler personuppgifter än vad som behövs för ändamålen.
- Ska se till att personuppgifterna är riktiga.
- Ska radera personuppgifterna när de inte längre behövs.
- Ska skydda personuppgifterna, till exempel så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs.
- Ska kunna visa att och hur ni lever upp till dataskyddsförordningen.

Exempel på personuppgifter:

- Ett namn och efternamn
- En hemadress
- En e-postadress såsom namn.efternamn@foretag.com
- Ett id-kortsnummer
- Platsinformation (t.ex. platsfunktionen på en mobiltelefon)
- En IP-adress
- Kakor
- Reklamidentifieraren på din telefon
- Uppgifter som innehas av ett sjukhus eller en läkare och som skulle kunna vara en symbol som fungerar som en unik identifikation av en person

### **1.6.2 Opt-in - aktivt medgivande**

GDPR kräver aktivt medgivande vilket innebär att varje person vars personuppgifter ska lagras ger aktivt samtycke till detta. Det innebär att de vars personuppgifter vi lagrar måste ge aktivt samtycke *innan* vi lagrar deras personuppgifter och att hen kan anses förstå innebörden av datalagringen.



Det räcker inte med att begära ett godkännande för att spara personuppgifterna utan man behöver även förklara varför och hur länge och hur de kommer att behandlas.

Några exempel:

- På anmälan till ett evenemang behöver det finnas en obligatorisk kryssruta där den som anmäler sig godkänner att dess personuppgifter sparas och behandlas av sektionen för att arrangemanget skall kunna genomföras eller för att personen skall kunna ta del av arrangemanget. Ytterligare skall personen informeras om varför och hur personuppgifterna behandlas och sparas. Exempel på text:

***För att arrangemanget ska gå att planera och genomföra behöver vi spara dina ovan angivna uppgifter under en begränsad tid. Dina personuppgifter kan komma att delas med tredje part, t.ex. puffar eller samarrangörer, om det behövs för arrangemanget. Strax efter arrangemanget kommer uppgifterna att raderas.***

- På puff-formulär vill spara arbetarnas uppgifter en längre tid än till strax efter arrangemangets slut. Anledningar till detta kan vara att man vill bjuda arbetarna på ett tackkalas eller be om hjälp vid senare tillfälle. Då kan följande stå:

***Dina uppgifter kommer att sparas för att vi ska kunna kontakta dig även vid senare tillfälle, t.ex. om vi behöver hjälp vid något annat arrangemang eller på något sätt vill tacka dig för din insats. Dina uppgifter kommer raderas vid slutet av vårt verksamhetsår.***

### **1.6.3 Tidsbestämt**

Uppgifter får inte sparas längre än nödvändigt. Några exempel:

- Anmälningslistor till sittningar skall raderas senast två veckor efter sittningen.
- Pufflistor skall raderas senast två veckor efter tackkalaset.

### **1.6.4 Specificitet**

En personuppgift får bara användas till det som den som äger personuppgiften har godkänt att den får användas till.

Antag att det finns ett godkännande för att spara e-postadresser för att kunna kontakta personer. Då är det endast okej för detta syfte och man får då inte använda dessa uppgifter för att skapa en mailinglista till alla som går på data eller dela uppgifterna till tredje part.

### **1.6.5 Spara alltid hela namnet**

Fullständigt namn ska alltid sparas tillsammans med andra personuppgifter för en person så att personuppgiftsansvarige har en rimlig möjlighet att t.ex. ta bort en persons personuppgifter om den vill bli bortglömd.

Det kan vara svårt att få deltagare att fylla i sina namn. Därför rekommenderar vi att fullständigt namn och smeknamn samlas in som separata fält för att uppmuntra de som fyller i listan eller formuläret att ge användbar information.



## 1.7 Shared Drive

Shared Drive är som en vanlig My Drive men det är gruppen och inte individerna som äger innehållet. Varje kommitté och förening får ha en och endast en TeamDrive som de ärver från tidigare år. För dessa gäller:

- Högst upp i mapphierarkin bör det finnas en mapp för varje år, t.ex. "2017" och "2018".
- Alla mappar och dokument döps så att en utomstående förstår vad det handlar om. Olämpliga namn kan vara "Supa satan mapp" och "Lite roligt bös". Döp dessa istället till "Postom" och "Förslag på arr" så följer ni policyn och gör livet lättare för era efterträdare.
- Alla dokument och mappar som innehåller personuppgifter ska ha ett namn med suffixet "[PU]" (PersonUppgifter). T.ex. mappen "Möten[PU]" eller filen "Kontaktuppgifter sittande[PU]".

Det är inte allt för sällan som man har ett gemensamt arrangemang med andra kommittéer eller puffar som behöver ta del av ett eller flera dokument.

- Om det är puffar som klarar sig med enstaka dokument, dela då endast dessa.
- Om det är ett samarr och utomstående/andra kommittéer behöver tillgång till alla filer är det okej att skapa en temporär Shared Drive dit man bjuder in alla arrangörer som behöver tillgång till filerna. Denna Shared Driven ska raderas alternativt ska allt innehåll flyttas efter arrangemanget om inte speciella omständigheter råder. Personuppgiftsansvarige beslutar om det råder speciella omständigheter. Ovanstående regler gäller även för dessa.

**Tips:** Om det är en hel grupp som ska ha tillgång till en drive räcker det med att gruppen bjuds in för att alla ska få tillgång.

**OBS!**Tänk på att ni måste ha godkännande att dela till tredje part, se Opt-in ovan. Intresseföreningar och kommittéer på data räknas inte som tredje part eftersom de är en del av datateknologsektionen.

- En mapp för varje år. T.ex. "2017", "2018".
- Det är okej att ha en mapp för alla år tidigare. T.ex. "1337–2016"

Vi rekommenderar att man följer ovanstående struktur för att göra det lätt för nya att snabbt få en överblick över vilka dokument som finns och var de ligger, men om den strukturen inte fungerar, använd en som fungerar bättre för er.

## 1.8 GMail

Använd enbart e-postadresserna du har genom sektionen till sektionsarbete, det är alltså både otillåtet och dumt att använda den för privat bruk då du lämnar över adressen till din efterträdare efter ditt verksamhetsår.

E-post får ej vidarebefordras till privata e-postadresser.

**Tips:** Sätt en signatur som automatiskt infogas i slutet av dina mejl. Förslag:

*Vänliga hälsningar,*

*<Förening> <Post> 20xx/20xx*



*Datateknologsektionen Chalmers Studentkår*  
*[www.dtek.se](http://www.dtek.se)**<**<http://www.dtek.se/>**>*

## **1.9 Kalender**

Man får gärna skapa en eller flera kalendrar. Viktigt är att tänka på sätta rätt åtkomsträttigheter och dela med rätt personer. Till exempel kan en bokningskalender som "databussen" eller "Basenpax", ha följande inställningar:

- Tillgänglig för alla: se endast ledig/upptagen (dölj uppgifter).
- Delad med: [dbus@dtek.se](mailto:dbus@dtek.se) respektive [alla@dtek.se](mailto:alla@dtek.se). Rätt att göra ändringar och hantera delning.

En intern kalender bör endast vara delad med kommittén och en kalender som delas med utomstående ska inte innehålla personuppgifter som de kan se.

Man kan lägga till hela grupper i en kalender, men då måste varje medlem lägga till kalendern via en länk som skickas till mejlen. Några bra kalendrar som finns som kan vara bra för alla datateknologer är:

- **Dtek-kalendern:**  
[https://calendar.google.com/calendar/embed?src=dtek.se\\_0tavt7qtqphv86l4stb0aj3j88%40group.calendar.google.com&ctz=Europe%2FStockholm](https://calendar.google.com/calendar/embed?src=dtek.se_0tavt7qtqphv86l4stb0aj3j88%40group.calendar.google.com&ctz=Europe%2FStockholm)
- **Basenpaxningar:**  
[https://calendar.google.com/calendar/embed?src=dtek.se\\_b3sv1v3upmtjquppg10hhe59e0%40group.calendar.google.com&ctz=Europe%2FStockholm](https://calendar.google.com/calendar/embed?src=dtek.se_b3sv1v3upmtjquppg10hhe59e0%40group.calendar.google.com&ctz=Europe%2FStockholm)
- **Databussen:**  
[https://calendar.google.com/calendar/embed?src=dtek.se\\_69sdfhe5527mh3u9tk9146imak%40group.calendar.google.com&ctz=Europe%2FStockholm](https://calendar.google.com/calendar/embed?src=dtek.se_69sdfhe5527mh3u9tk9146imak%40group.calendar.google.com&ctz=Europe%2FStockholm)

## **1.10 Handlingsplan vid dataläcka**

Vid minsta misstanke om dataläcka, kontakta omedelbart personuppgiftsansvarig i Styrelsen: [Styrelsen@dtek.se](mailto:Styrelsen@dtek.se).