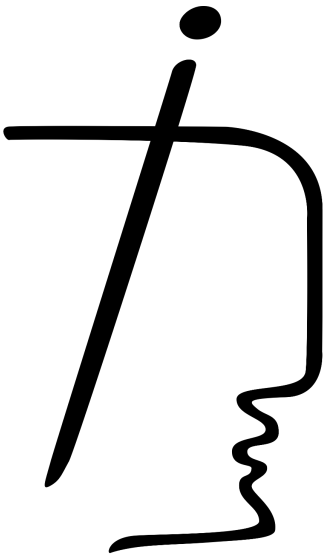

INDUSTRIELL EKONOMI
KUNGLIGA TEKNISKA HÖGSKOLAN

# GDPR-policy

Utfärdad: 2021-11-24

# Bakgrund

I enlighet med Dataskyddsförordningen som trädde i kraft i maj 2018 ska alla organisationer skydda personuppgifter, samt göra det enkelt för individer att veta vilka uppgifter som registreras, hanteras och lagras hos organisationen. Lagen, vidare benämnd som GDPR, ställer krav på att sektionen behandlar personuppgifter på ett strukturerat och säkert sätt.
Sektionen ska vidare också förhålla sig till de regler och styrdokument uppsatta av THS.

Detta dokument är ett komplement till motsvarande GDPR-policydokument utfärdat av THS, och ämnar att förtydliga och hjälpa till i den praktiska tillämpningen av GDPR-policyn. Det ska även förtydliga rutiner kring insamlande av uppgifter, hantering av dessa samt utlämning av uppgifter till tredje part.

Dataskyddsförordningen går att läsa i sin helhet här (GDPR).

# Syfte

Sektionens syfte är att bidra med studentnytta i form av gemenskap och kompetensutveckling, och för att bedriva den verksamheten krävs vissa typer av personuppgifter. All insamling av personuppgifter ska ha ett tydligt, specifikt och berättigat ändamål och det är ändamålet som begränsar vilka uppgifter som får samlas in, behandlas samt hur länge de får lagras.

### GDPRs grundläggande principer

Personuppgiftsansvariga, dvs sektionen:

- Måste ha stöd i GDPR för att få behandla personuppgifter
- Får endast samla in uppgifter till specifika, särskilt angivna, berättigade ändamål
- Ska inte behandla fler uppgifter är nödvändigt för ändamålet
- Ska se till att uppgifterna är riktiga
- Ska radera uppgifterna så fort de inte längre behövs
- Ska skydda uppgifterna så att obehöriga ej kan ta del av dem, samt att de ej förloras eller förstörs
- Ska kunna visa hur de lever upp till GDPR.

# Insamling av uppgifter

Insamling av uppgifter kan ske bland annat i samband med sektionsevenemang eller genom att sektionen begär information av THS. Även de uppgifter sektionen insamlat via THS ska hanteras i enlighet med detta dokument.

Med personuppgift gäller all information som kan knytas till en fysisk person. Uppgifter som omfattas av GDPR som samlas in av sektionen är till exempel, men begränsas inte nödvändigtvis till:

- Namn
- Adress
- Årskurs
- Medlemskap
- Matpreferens
- Bild på identifierbar person
- Telefonnummer
- Mailadress
- Personnummer
- Nämndpreferenser
- Kandidaturer till förtroendevalda poster

Information om enskilda näringsidkare och kontaktpersoner från företag räknas som personuppgifter, information om juridiska personer gör inte det.

Insamling av personuppgifter ska ske i den utsträckning det är nödvändigt och syftet ska tydligt framgå. Det ska vara tydligt för både den som samlar in uppgifter och den som delar sina uppgifter vem som har tillgång till uppgifterna och hur länge de lagras, samt till vad de ska användas.

### Temporära uppgifter

Insamling av temporära uppgifter till event och liknande, får samlas in av en sektionsmedlem med ansvar delegerat av en förtroendevald. Det ska för varje event finnas en person ansvarig för insamlandet, hanterandet samt raderandet av uppgifterna.

### Långsiktiga uppgifter

Långsiktiga uppgifter som medlemsregister eller nyantagna studenter ska insamlas av Styrelsen eller annan person med ansvar delegerat av styrelsen. Bilder från sektionsevent räknas också som långsiktiga uppgifter och insamlas av Kommunikationsnämnden.

Rätt:
Estiem anordnar Destination X och ber om personuppgifter såsom namn, personnummer, telefonnummer och mailadress. Syftet framgår tydligt i OSAn att det är för att hantera bokningar i resenärernas namn och andra evenemang under resan.

Fel:
Kulturnämnden anordnar tunnelbanesittningen och ber om namn, adress, mailadress och telefonnummer i OSAn, eftersom de inte ännu vet vilka uppgifter de kommer behöva för att anordna eventet, och ber om uppgifter “i fall att” de kommer behövas.

# Lagring av uppgifter

Vilka uppgifter som samlas in av sektionen ska tydligt framgå i en förteckning. Uppgifter ska lagras på ett sådant sätt att ingen obehörig får tillgång till dem, förslagsvis med lösenordsskydd, och det är varje enskild persons ansvar att personuppgifter skyddas. Skyddet ska anpassas till uppgiftens känslighet. Kan personuppgifterna räknas som känsliga räcker inte lösenord/lösenkod till dator eller telefon som enda säkerhetsåtgärd.

Temporära uppgifter ska raderas när dess syfte uppnåtts.

Långsiktiga uppgifter ska lagras i enlighet med den **rättsliga grund** sektionen innehar för vederbörande uppgift, tex genom samtycke, intresseavvägning eller avtal. Tiden för lagringen ska också framgå i förteckningen, och ansvaret att detta följs åligger den person som samlar in uppgiften. Med samtycke som rättslig grund måste även samtycket sparas så länge uppgiften sparas.

Uppgifter kan anonymiseras i syfte att föra statistik. Uppgifter får då lagras om de skapats så att de inte går att återskapa till sitt original och är omöjliga att koppla till en person.

Om man tagit del av personuppgifter via mail räknas det som lagring av personuppgift och måste därmed hanteras på liknande sätt som om uppgiften hämtats på ett annat sätt. Uppgifterna ska då överföras till ett lämpligt, bättre skyddat lagringsutrymme och mailet ska raderas. Sektionen ska i största möjliga mån undvika att begära personuppgifter via mail.

Rätt:
Estiem anordnar Destination X och använder insamlade personuppgifter för att boka biljetter och andra evenemang under resan. När alla deltagare kommit hem från resan raderas alla personuppgifter.
Under resan ligger personuppgifterna sparade i en lösenordsskyddad fil på en av arrangörernas telefon.

Fel:
Spexet anordnar GD och ber om namn, mailadress och matpreferens genom ett google-formulär. De sparar personuppgifterna till nästa GD några veckor senare.
Uppgifterna hanteras inte som långsiktiga och de lagras endast i svarsdelen av formuläret.

# Hantering av uppgifter

Personuppgifter får endast användas till det syftet som uppgifterna lämnades för.
Det ska alltid vara möjligt för en person att begära ut de uppgifter sektionen innehar om personen och, om så önskas, begära att dessa uppgifter **raderas**. Det innefattar även att avregistrera sig på mailutskick eller liknande “prenumerationer”.

### Publikation

Alla uppgifter som publiceras på sektionens officiella kanaler berörs av GDPR. I vissa fall, då anledningen till publiceringen kan antas vara självklar, får sektionen publicera personuppgifter utan medgivande, men man bör alltid informera om en publiceringen.
Om sektionens intresse överstiger det intresse den enskilda individens intresse av skydd av sina uppgifter får publicering ske utan uttryckt samtycke, hanteringen ska dock alltid kunna härledas från en intresseavvägning.

Publicering får också ske med uttryckt samtycke. Det måste då vara möjligt att ge samtycke till all hantering av personuppgifter separat från andra godkännanden, dvs man får inte paketera godkännande av hantering av personuppgifter tillsammans med andra icke nödvändiga uppgifter. Möjligheten att ångra sig utan att lida negativa konsekvenser måste också finnas och är detta inte möjligt bör en annan rättslig grund tillämpas.

I dessa fall måste även samtycket att publicera lagras så länge uppgiften är publik, då ska hur, när och vilken information som gavs vid tillfället sparas.

För bilder gäller att bilden är en personuppgift för alla identifierbara personer på fotot. Det innebär även personer i bakgrunden. För publicering av personuppgift i form av bild används generellt intresseavvägning som rättslig grund. Publiceringen sker på sektionens Facebook-sida *Sektionen för Industriell Ekonomi KTH* samt sektionens instagram *isektionen_kth*. För varje publicering avvägs om sektionens intressen väger tyngre än den registrerades. Sektionens intressen är att uppmärksamma sektionens verksamhet för tredje part, så som framtida I-studenter, I-studenter som inte deltog på eventet eller studenter från annan sektion, och på det sättet öka populariteten på eventen, samt att ge de närvarande möjlighet att ta del av uppgifterna för eget nöje och stärka sammanhållningen på sektionen.

Inför varje event där bilder tas som personuppgift ska det framgå i OSA, eventinformation och/eller på plats att bilder tas och möjlighet ska finnas att be ansvarig att ej ta bild på vederbörande. Vid publikation på FaceBook-sidan *Sektionen för Industriell Ekonomi KTH* ska det i samband med publikation alltid stå att bilder tas bort på begäran och begäran skickas då till Facebook-sidan. Samma sak gäller vid publicering på Instagram om bilden publiceras med intresseavvägning och begäran om att ta bort bild skickas som meddelande till sektionens konto.

Rätt:
Kommunikationsnämnden skickar regelbundet ut nyhetsbrev och blir ombedda att avregistrera en medlem. Kommunikationsnämnden tar då bort personen från maillistan, och tar bort alla uppgifter om personen som är lämnade i syftet att skicka nyhetsbrev.

Fel:
En person ber kommunikationsansvarig att få veta vilka uppgifter sektionen har sparat om den. Sektionen har ingen uppgiftsförteckning och vet inte vilka av dennes personuppgifter som finns på och hanteras av sektionen.

Fel:
Dagen-I bokar företag till sin mässa och ber, genom en kryssruta, att de godkänner att Dagen-I hanterar personuppgifter om enskilda företagsrepresentanter och samtidigt godkänna de avtalsvillkor som presenterats tidigare. Detta kallas alltså paketering och är inte tillåtet.

# Utlämning av uppgifter till tredje part

Sektionen är ansvarig för alla uppgifter som delas ut och de uppgifter som lämnas ut får endast användas i enlighet med gällande lagar samt detta och av THS motsvarande policydokument. Det innebär att uppgifter endast får lämnas ut till aktörer som kan garantera att uppgifterna hanteras enligt GDPR.

Sektionen får lämna ut uppgifter till tredje part om vi säkert vet till vad och varför de ska användas, samt säkerställt att de verkligen är nödvändiga. Sektionen måste också säkerställa att utlämnandet är motiverat.

## Uppgiftsförteckning

Ett exempel på hur uppgiftsförteckningen kommer se ut

| Syfte | Typ av uppgifter | Lagringstid | Typ av behandling | Rättslig grund |
|---|---|---|---|---|
| | Namn<br>Adress<br>... | | | |
| | | | | |
| | | | | |
| | | | | |

# Förklaring av begrepp

*Rättslig grund innebär det som styrker en organisations rätt att hantera personuppgifter. Samtycke som rättslig grund innebär att en uppgift har lämnats med **frivilligt aktivt samtycke**. Avtal som rättslig grund innebär att en person har eller ska ingå ett avtal med sektionen och genomförandet kräver vissa uppgifter. Fler rättsliga grunder finns att läsa om på Datainspektionens hemsida.*

*Att en uppgift raderas innebär att den tas bort så att den inte kan återskapas.*