# \\dustaff\home\aac\Windesk\hd_rgb300dpi-max.jpg

#

**Checklista för IT-tjänster som behandlar personuppgifter**

Genom att gå igenom punkterna i den här checklistan kan du kontrollera om IT-tjänsten lever upp till de krav som ställs vid behandling av personuppgifter. Har du därefter frågor kan du kontakta högskolans dataskyddsombud. Innan du använder checklistan bör du ta del av högskolans information på webben om behandling av personuppgifter.

 **Innan behandling påbörjas**

1. **Personuppgifter**: Kommer personuppgifter (uppgifter som på något sätt går att koppla till en person som är i livet) att behandlas i tjänsten?

*Personuppgifter ska bara behandlas om det är nödvändigt. Går det istället att använda anonyma uppgifter? Om uppgifterna är anonyma och inte på något sätt kan kopplas till person omfattas de inte av dataskyddsförordningen och du behöver inte använda dig av checklistan. Observera att kodade personuppgifter omfattas av dataskyddsförordningen så länge det finns en kodnyckel.*

* **Känsliga personuppgifter eller extra skyddsvärda personuppgifter**: Kommer känsliga personuppgifter behandlas? D.v.s. uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, hälsa, sexualliv eller sexuella läggning, genetiska uppgifter eller biometriska uppgifter. Kommer extra skyddsvärda personuppgifter att behandlas? Så som till exempel personnummer, vissa uppgifter om lön, skyddade personuppgifter, sekretessbelagda uppgifter, uppgifter om lagöverträdelser, uppgifter om sociala förhållanden, uppgifter som ligger nära den privata sfären, beskrivningar och värderingar av personliga egenskaper.

*Ställer större krav på hanteringen. Går det istället att uppnå samma ändamål med anonyma uppgifter? Se ovan.*

1. **Rättslig grund**: Vilken rättslig grund kommer behandlingen baseras på?

*T.ex. avtal, rättslig förpliktelse, myndighetsutövning, allmänt intresse eller samtycke.*

1. **Information**: Är de registrerade informerade i enlighet med kraven i dataskyddsförordningen?

*Följande ska framgå: Ändamål med behandlingen (t.ex. utbildning, forskning eller samverkan), rättslig grund för behandlingen (t.ex. avtal, myndighetsutövning, allmänt intresse), vilka som kommer kunna ta del av uppgifterna (t.ex. medarbetare, studenter, allmänheten, andra myndigheter), hur länge uppgifterna sparas (t.ex. så länge de behövs för ändamålet och så länge som krävs enligt lagar och andra föreskrifter), rätten för deltagare att få tillgång till uppgifterna och få fel rättade, rätten för deltagare att återkalla samtycke, att Högskolan Dalarna är personuppgiftsansvarig, kontaktuppgifter till dataskyddsombudet på högskolan (**dataskydd@du.se**), deltagarnas rätt att framföra klagomål till Integritetsskyddsmyndigheten, IMY.*

1. **Ändamålsbegränsning**: Behandlas uppgifterna för särskilda, uttryckligt angivna och berättigade ändamål?
2. **Uppgiftsminimering**: Är ﻿uppgifterna adekvata, relevanta och inte för omfattande i förhållande till ändamålet?
3. **Lagringsminimering**: Hur länge ska uppgifterna lagras för ändamålet?

*Personuppgifter får lagras så länge de behövs för ändamålet och så länge som krävs enligt lagar och andra föreskrifter. Kontakta arkivfunktionen vid frågor om bevarande/gallring (**arkiv@du.se**).*

1. **Överföring till tredje land**: Kommer uppgifter överföras utanför EU/EES?

*Det är bara tillåtet i vissa fall. Kontakta dataskyddsombudet innan eventuell överföring påbörjas (**dataskydd@du.se**).*

1. **Personuppgiftsbiträde**: Kommer tredje part att behandla personuppgifterna? T.ex. en leverantör av en IT-tjänst?

*Kontakta dataskyddsombudet innan eventuellt avtal undertecknas (**dataskydd@du.se**).*

1. **Riskanalys**: Har riskanalys gjorts och dokumenterats?

*Analysera riskerna med behandlingen och dokumentera dina slutsatser, t.ex. som en del av systemdokumentationen.*

1. **Säkerhetsåtgärder**: Har nödvändiga säkerhetsåtgärder vidtagits baserat på riskanalysen, och har dessa åtgärder dokumenterats, t.ex. i systemdokumentationen?
2. **Konsekvensbedömning och förhandssamråd**: Visar genomförd riskanalys att det behövs en konsekvensbedömning eller förhandssamråd på grund av särskilt allvarliga risker för de registrerade? Dataskyddsombudet finns i så fall tillgängligt för råd och stöd.
3. **Anmälan**﻿﻿: Är behandlingen anmäld till dataskyddsombudet via avsedd digital blankett *”Anmälan av behandling av personuppgifter i verksamhetssystem”*?
Den digitala blanketten återfinns på högskolan webb.

*Anledningen till anmälningskravet är att högskolan enligt dataskyddsförordningen är skyldig att föra ett register över alla pågående behandlingar på högskolan. För att kunna leva upp till detta behöver ombudet få in anmälan.*

**Under behandling**

1. **Korrekthet**: Säkerställ att behandlade uppgifter korrekta. Finns rutiner för detta?
2. **Registrerades rättigheter**: Hantera eventuell begäran från deltagare om att tillvarata sina rättigheter, t.ex. återtagande av samtycke. Kontakta dataskyddsombudet vid frågor eller om begäran gäller andra rättigheter, t.ex. registerutdrag (dataskydd@du.se).
3. **Personuppgiftsincidenter**: Rapportera snarast eventuella personuppgiftsincidenter, t.ex. förlust av uppgifter eller risk för obehörig åtkomst till uppgifter, till support@du.se.

**Efter behandling**

1. **Avsluta behandling**: Avidentifiera, arkivera eller radera (gallra) uppgifterna i enlighet med gällande föreskrifter. Kontakta arkivfunktionen vid frågor (arkiv@du.se).
2. **Avanmälan**: Meddela dataskyddsombudet när behandlingen upphör via avsedd digital blankett *”Ändring eller avanmälan gällande behandlingen”*.
Den digitala blanketten återfinns på högskolans webb.