Riktlinje
2022-08-30
Ärendenr: ORU 2020/05382
Sidnr: 1 (4)

Riktlinjer för Örebro universitets behandlingar av personuppgifter

Ledning och styrning av arbetet med GDPR vid Örebro universitet

Dokumentet beskriver Örebro universitets organisation, ansvar och de grundläggande principerna för behandling av personuppgifter. Stöd och vägledning för hur personuppgiftsbehandling ska gå till i det dagliga arbetet presenteras på intranätet under GDPR eller på Integritetsskyddsmyndigheten hemsida.

Dataskyddsförordningens (GDPR) grunder

GDPR (EU) 2016/679 gäller som lag i alla EU:s medlemsländer från och med den 25 maj 2018.

De grundläggande dataskyddsprinciperna innebär:

- Laglighet – att alla behandlingar av personuppgifter måste ha stöd i lag eller förordning.
- Ändamålsbegränsning – att bara samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål.
- Uppgiftsminimering – att inte behandla fler personuppgifter än vad som behövs för ändamålen.
- Riktighet – att se till att personuppgifterna är riktiga.
- Lagringsminimering – att radera personuppgifter när de inte längre behövs (gallra/arkivera).
- Integritet – att skydda personuppgifterna, tillse att obehörig ej får tillgång, att uppgifter förloras eller förstörs.
- Ansvarsskyldighet – att inte bara följa utan även kunna visa att och hur man lever upp till GDPR.

De rättsliga grunder Örebro universitet (ORU) kan ha som stöd för en personuppgiftsbehandling för sin verksamhet är följande: **Rättslig förpliktelse**, **Myndighetsutövning**, **Allmänt intresse**, **Nödvändigt för avtal** och **Samtycke**.

En riskanalys för användning av personuppgifter ska genomföras inför varje ny behandling, där dataskyddsprincipernas punkter ska besvaras.

GDPR och andra lagar

GDPR hindrar inte den personuppgiftsbehandling som är nödvändig enligt verksamhetsreglerad lagstiftning, föreskrifter eller för att myndigheter ska kunna uppfylla skyldigheten enligt arkivlagen eller att lämna ut allmänna handlingar enligt offentlighetsprincipen.

Registerförteckning (sammanställning av verksamhetens personuppgiftsbehandlingar)

Örebro universitetet har en legal skyldighet att förteckna sina personuppgiftsbehandlingar. Det finns en registerförteckning som till stor del utgår från beskrivningen av universitetets processer som återfinns i informationshanteringsplanen. I förteckningen framgår bl.a. en beskrivning av processgruppen, ändamål, personkategori och vilka personuppgifter som används samt rättslig grund.

Varje avdelning och institution ska kontrollera att de personuppgiftsbehandlingar som sker i verksamheten går att återfinna i registerförteckningen. Om en behandling saknas ska dataskyddsombudet kontaktas för hjälp med dokumentation.

Ansvarsfördelning

Personuppgiftsansvarig är Örebro universitet för personuppgiftsbehandlingar vid myndigheten. Ansvaret gäller även för personuppgiftsbehandlingar för den forskning som genomförs inom ramen för universitetets verksamhet samt behandlingar utförda av studenter inom ramen för sina studier.

Prefekt/avdelningschef ansvarar för att reglerna för personuppgiftsbehandling följs inom det egna verksamhetsområdet. Prefekt/avdelningschef är dataskyddssamordnare vid institutionen/avdelningen. Uppgiften kan delegeras och fördelas mellan institutionerna och mellan avdelningarna.

Systemägare ansvarar för att ett system där personuppgifter behandlas är förenligt med de krav som ställs enligt GDPR. Som system räknas även inköpta systemtjänster som inte driftas av Örebro universitet. Systemägare ansvarar för att frågorna avseende dataskydd besvaras och dokumenteras i SystemInventeringsLista vid Örebro universitet (SILOU).

Nyttjare av system/tjänst/process ansvarar för att den behandling av personuppgifter som denne utför sker i enlighet med de krav som ställs enligt GDPR.

Medarbetare ansvarar för att känna till och förhålla sig till GDPR inom ramen för sin aktuella verksamhet, att bara nyttja av ORU godkända system och tjänster vid behandling av personuppgifter samt att självständigt söka svar på frågor gällande dataskydd utifrån den information som finns på intranätet. Om frågan saknar svar, kan den ställas till centrala verksamhetsstödet (arkiv, informationssäkerhet, dataskyddsombud, juridik).

Forskare ansvarar för att känna till och förhålla sig till GDPR samt fastställda rutiner för forskning innehållande personuppgifter. Huvudansvarig forskare för ett projekt ansvarar för att nödvändiga avtal gällande GDPR är tecknade och registrerade, att riskanalys och eventuell konsekvensbedömning är genomförd m.m. För alla forskningsprojekt som behandlar personuppgifter ska det finnas dokumenterat att datasskyddsprinciperna har beaktats och på vilket sätt.

Lärare/kurs-/programansvarig ansvarar för att informera om och hänvisa studenter till information om GDPR när personuppgifter är nödvändiga för att uppfylla utbildningsmålen. Riktad information till studenterna finns tillgänglig via oru.se. För alla studentarbeten som behandlar personuppgifter ska det finnas dokumenterat att datasskyddsprinciperna har beaktats och på vilket sätt.

Student ansvarar för att känna till och förhålla sig till GDPR inom ramen för sina studier i enlighet med den information de fått från universitetet.

Dataskyddsombud (DSO)

Den övergripande och viktigaste uppgiften för DSO är att verka för att organisationen följer GDPR. Det innebär bland annat att:

- informera, utbilda och ge råd inom organisationen,
- kontrollera att organisationen följer bestämmelser och interna styrdokument.

DSO ska också:

- ge råd om riskanalyser och konsekvensbedömningar,
- vara kontaktperson för de registrerade och personalen inom organisationen,
- vara kontaktperson för Integritetsskyddsmyndigheten och samarbeta med denna vid exempelvis incidenter och inspektioner.

DSO lämnar en rapport årligen till universitetsstyrelsen. DSO avrapporterar det löpande arbetet gällande verksamhetens efterlevnad av GDPR till chefen för Universitetskansliet.

Kontaktuppgift till DSO är dataskyddsombud@oru.se.

Dataskyddssamordnare vid avdelning och institution

Uppgifter om vem som är dataskyddsamordnare finns publicerat på intranätet under GDPR.

Dataskyddssamordnaren har till uppgift att:

- ansvara för att ta fram uppgifter till DSO vid registerförfrågan och begäran från enskild enligt GDPR
- rapporterar till DSO (vid begäran om registerutdrag)
- vid en personuppgiftsincident, delta som stöd till den ansvarige för behandlingen (ex. systemägare) i utredning och hantering av incidenten utifrån den kompetens som DSS ges avseende dataskydd via universitetets utbildningar,
- sprider centralt framtagen/given information i den egna verksamheten avseende GDPR/personuppgiftshantering,
- informera vid sin avdelning/institution om hantering av personuppgifter i de fall denna hantering avviker från centralt framtagna dokument eller om egna rutiner utifrån dessa dokument har arbetats fram tillsammans med dataskyddssamordnaren,
- samordnar verksamhetens hantering av personuppgiftsbehandlingar i de fall dessa inte framgår av registerförteckningen (se ”Registerförteckning” ovan),
- medverkar i nätverket för dataskyddssamordnare vid Örebro universitet för utveckling av arbetet med dataskyddsfrågor,
- är kontaktperson till DSO.

Fördjupad rådgivning, komplexa frågor, avtalsregleringar etc. hänvisas till centrala verksamhetsstödet (DSO/arkiv/informationssäkerhet/juridik)

Personuppgiftsbiträde

Hanterar personuppgifter för Örebro universitets räkning på instruktion från universitet efter skriftligt avtal.

Skyldighet att informera

Örebro universitet är skyldigt att informera de registrerade om hur persondata kommer att behandlas enligt GDPR, hur den registrerade tillvaratar sina rättigheter m.m.

Detta görs övergripande i Örebro universitet dataskyddspolicy som finns publicerad på Örebro universitets hemsida. Utöver det ska varje process/system/tjänst vid Örebro universitet tillhandahålla information om hur personuppgifter behandlas. Information ska även delges vid annan inhämtning, ex blanketter, inspelning av föreläsningar, sociala medier m.m.

Personuppgiftsincidenter

Den som ansvarar för personuppgifter är skyldig att ha rutiner för att kunna upptäcka, utreda och rapportera personuppgiftsincidenter. Den som är ansvarig för den aktuella behandlingen ska omedelbart efter att en överträdelse upptäckts anmäla detta till DSO och påbörja en utredning med en risk- och konsekvensbedömning. Enskilda personer som upptäcker eller misstänker att en personuppgiftsincident skett anmäler detta direkt till DSO.

Om anmälan ska ske till Integritetsskyddsmyndigheten ska denna göras inom 72 timmar från att incidenten kommit till myndighetens kännedom. Alla incidenter med utredning ska registreras vid Örebro universitet, detta sker i Public 360.