Dataskydd/GDPR

Styrdokument Örebro universitet
Kategori: Riktlinjer
Ärendenummer: ORU 2024/02826
Beslutsfattare: Rektor
Senast ändrad: 2024-05-21
Fastställd: 2022-08-30
Dokumentansvarig: Rättskansliet

Innehåll

Inledning

Dokumentet beskriver Örebro universitets organisation, ansvar och de grundläggande principerna för dataskydd/GDPR. Stöd och vägledning för hur personuppgiftsbehandling ska gå till i det dagliga arbetet finns på intranätet Inforum.

Riktlinjerna bygger på EU:s dataskyddsförordning som implementerats till svensk lag. 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, se till att obehörig ej får tillgång, samt att uppgifter förloras eller förstörs.
- Ansvarsskyldighet – att inte bara följa, utan även kunna visa att och hur man lever upp till dataskydd/GDPR.

Dataskydd/GDPR vid Örebro universitet

All personuppgiftsbehandling måste stödja sig på någon av de rättsliga grunderna för att vara laglig. De rättsliga grunder som universitet kan ha som stöd för en personuppgiftsbehandling i verksamheten är följande:

- Rättslig förpliktelse – det finns lagar och regler som gör att personuppgiftsansvarig måste behandla vissa personuppgifter i sin verksamhet.
- Myndighetsutövning – personuppgiftsansvarig måste behandla personuppgifter för att utföra sina myndighetsuppgifter på statens uppdrag.
- Allmänt intresse – personuppgiftsansvarig måste behandla personuppgifter för att utföra uppgift av allmänt intresse som har stöd i lag eller annan författning. Exempelvis så som utbildning och forskning.
- Nödvändigt för avtal – personuppgiftsbehandling som kan vara nödvändig för att fullfölja ett avtal, exempelvis personaladministrativa system.
- Samtycke – som regel kan inte samtycke använda som rättslig grund för anställda och studenter, då de står i beroendeställning till universitetet.

Intresseavvägning – personuppgiftsansvarigas intressen väger tyngre än den registrerades och om behandlingen är nödvändig för det aktuella ändamålet. Universitetet får dock som myndighet inte tillämpa intresseavvägning som rättslig grund.

Universitetet ska förteckna sina personuppgiftsbehandlingar. Det finns en registerförteckning som till stor del utgår från beskrivningen av universitetets processer som återfinns i informationshanteringsplanen. Av registerförteckningen framgår bland annat 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. För de personuppgiftsbehandlingar som är specifika för en enskild avdelning eller institution ska de specifika omständigheterna dokumenteras av verksamheten. Dessa redovisas till dataskyddsombudet som sammanställer Örebro universitet gemensamma registerförteckning.

En riskanalys för användning av personuppgifter ska genomföras där dataskyddsprincipernas punkter besvaras inför varje ny behandling som inte redan finns upptagen i Örebro universitets registerförteckning och/eller i informationshanteringsplanen.

Dataskydd/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.

Universitet ska informera de registrerade om hur persondata kommer att behandlas enligt GDPR, hur den registrerade tillvaratar sina rättigheter med mera. Detta görs övergripande i universitets dataskyddspolicy som finns publicerad på oru.se. Utöver det ska varje process/system/tjänst vid universitet tillhandahålla information om hur personuppgifter behandlas. Information ska även delges vid annan inhämtning, till exempel via blanketter, inspelning av föreläsningar, sociala medier.

Roller och ansvar

Örebro universitet är personuppgiftsansvarig för alla personuppgiftsbehandlingar vid myndigheten. Ansvaret gäller även för personuppgiftsbehandlingar inom forskning som genomförs inom ramen för universitetets verksamhet samt behandlingar utförda av studenter inom ramen för sina studier. Olika roller har olika ansvarsområden inom dataskydd/GDPR.

Dataskyddsombud

Enligt lag ska universitet ha ett dataskyddsombud (DSO) utnämnt. Den övergripande och viktigaste uppgiften för dataskyddsombudet är att verka för att organisationen följer dataskydd/GDPR. Det innebär bland annat att:

- informera, utbilda och ge råd inom organisationen om bland annat riskanalyser och konsekvensbedömningar
- kontrollera att organisationen följer bestämmelser och interna styrdokument
- vara kontaktperson för de registrerade och anställda inom organisationen
- vara kontaktperson för Integritetsskyddsmyndigheten och samarbeta med denna vid exempelvis incidenter och inspektioner
- årligen lämna en rapport om dataskyddsarbetet till universitetsstyrelsen

Dataskyddssamordnare vid avdelning och institution

Varje avdelning och institution ska ha en dataskyddssamordnare (DSS). Uppgifter om vem som är dataskyddssamordnare finns publicerat på Inforum. Uppgiften kan delegeras och fördelas mellan institutionerna och mellan avdelningarna.

Dataskyddssamordnaren har till uppgift att:

- ansvara för att ta fram uppgifter till DSO vid registerförfrågan och begäran från enskild
- rapportera till DSO (vid begäran om registerutdrag)
- vid en personuppgiftsincident, delta som stöd till den ansvarige för behandlingen (till exempel systemägare) i utredning och hantering av incidenten utifrån den kompetens som dataskyddssamordnare ges avseende dataskydd via universitetets utbildningar
- sprida centralt framtagen/given information i den egna verksamheten avseende dataskydd/GDPR
- informera vid sin avdelning/institution om dataskydd/GDPR i de fall denna hantering avviker från centralt framställda dokument eller om egna rutiner utifrån dessa dokument har arbetats fram tillsammans med dataskyddssamordnaren,
- samordna verksamhetens hantering av personuppgiftsbehandlingar i de fall dessa inte framgår av registerförteckningen
- medverka i nätverket för dataskyddssamordnare vid universitetet för utveckling av arbetet med dataskydd/GDPR
- vara kontaktperson till DSO

Fördjupad rådgivning, komplexa frågor, avtalsregleringar etc. hänvisas till centrala verksamhetsstödet (DSO/arkiv/informationssäkerhet/juridik). För forskning finns även forskningsdatarådgivare på varje fakultet.

Personuppgiftsbiträde

Ett personuppgiftsbiträde (PUBA) hanterar personuppgifter för Örebro universitets räkning på instruktion från universitet efter skriftligt avtal.

Övriga roller

Prefekt/avdelningschef ansvarar för att reglerna för personuppgiftsbehandling följs inom det egna verksamhetsområdet och för att vid behov ta fram egna rutiner för verksamhetens specifika behandlingar. Prefekt/avdelningschef är dataskyddssamordnare vid institutionen/avdelningen. Uppgiften som dataskyddssamordnare kan delegeras och fördelas mellan institutionerna och mellan avdelningarna.

Systemägare som ansvarar för ett system där personuppgifter behandlas ska se till att dataskydd/GDPR uppfylls. Som system räknas även inköpta systemtjänster som inte driftsätts av universitetet. Systemägare ansvarar för att frågorna avseende dataskydd besvaras och dokumenteras på vid angivet sätt vid universitetet.

Informationsägare som ansvarar för processer där personuppgifter behandlas ska se till att dataskydd/GDPR uppfylls. Informationsägare ansvarar för att frågorna avseende dataskydd besvaras och dokumenteras på angivet sätt vid universitetet.

Nyttjare av system/tjänst/process ansvarar för att den behandling av personuppgifter som denne utför sker i enlighet med de krav som ställs enligt dataskydd/GDPR samt riktlinjer och rutiner vid universitetet.

Medarbetare ansvarar för att känna till och förhålla sig till dataskydd/GDPR inom ramen för sin aktuella verksamhet, att bara nyttja av universitetet godkända system och tjänster vid behandling av personuppgifter samt att självständigt söka svar på frågor gällande dataskydd utifrån den information som finns på intranätet och hos stödfunktioner.

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

Lärare, kurs- och programansvariga ansvarar för att informera om och anvisa studenter till information om dataskydd/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 dataskydd/GDPR har beaktats och på vilket sätt.

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