DATASKYDDSFÖRORDNINGEN (GDPR)

Information för dig som jobbar med utbildning och administration

UMEÅ UNIVERSITET

VAD ÄR GDPR?

Dataskyddsförordningen (GDPR - The General Data Protection Regulation) är en **EU-förordning** som gäller som **svensk lag.**

Lagen trädde i kraft den 25 maj 2018.

Samma lag gäller inom hela EU.

Lagen är till för att skydda enskildas grundläggande rättigheter och friheter, särskilt deras rätt till skydd av personuppgifter.

EU-nivå

DATASKYDDSFÖRORDNINGEN (GDPR)

Nationell nivå

DATASKYDDSLAGEN REGISTERFÖRFATTNINGAR

I Sverige kompletteras dataskyddsförordningen av dataskyddslagen och andra registerförfattningar.

UMEÅ UNIVERSITET

UTGÅNGSPUNKTER

- Utgångspunkten i dataskyddsförordningen är att den enskilde personen äger sina egna personuppgifter.
- Andra får endast behandla uppgifterna om man har fått lov från den enskilde (samtycke) eller har annan laglig grund för behandlingen.
- Innan behandling måste det därför säkerställas att det finns en rätt att hantera personuppgifterna.
- Sedan måste behandlingen ske i enlighet med gällande regler och instruktioner.

NÄR GÄLLER GDPR?

- GDPR gäller för sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg (alltid om uppgifterna finns i datorn).
- Kopplar man personuppgifter som finns på pappershandlingar till ett digitalt sökbart register ”smittar” registret av sig på pappersuppgifterna och GDPR blir tillämpligt.
- GDPR gäller också helt manuell behandling av personuppgifter om personuppgifterna ingår eller är avsedda att ingå i ett register som är sökbart enligt särskilda kriterier (ibland om uppgifterna finns på papper)

VAD HÄNDER OM MAN INTE FÖLJER GDPR?

Allmänhetens förtroende för universitetet och vår verksamhet skadas.

Datainspektionens verktyg

- Tillsyn, föreläggande, varning och reprimand
- Administrativa sanktionsavgifter - för myndigheter högst 10 miljoner kronor

Den registrerades egna möjligheter

- Lämna in klagomål till Datainspektionen
- Begära skadestånd

GRUNDLÄGGANDE BEGREPP

- Den registrerade
- Personuppgifter
- Behandling
- Personuppgiftsansvarig
- Personuppgiftsbiträde
- Känsliga personuppgifter

PERSONUPPGIFTER

”Varje upplysning som avser en **identifierad** eller **identifierbar** fysisk person (den registrerade)”

Personnummer, namn, e-postadress, IP-nummer och cookies, bilder och ljudupptagningar, inlägg på sociala medier, inloggningsuppgifter, telefonnummer, adresser m.m.

Avgörande är om uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en levande person.

- Kodade, krypterade eller pseudonymiserade uppgifter som kan hänföras till en fysisk person med hjälp av kompletterande uppgifter = personuppgifter.
- Helt anonymiserade personuppgifter = **inte** personuppgifter

BEHANDLING AV PERSONUPPGIFTER

Alla former av åtgärder med personuppgifter är personuppgiftsbehandling, till exempel:

- insamling
- registrering
- organisering
- strukturering
- lagring
- bearbetning
- ändring
- framtagning
- läsning
- användning
- utlämning
- spridning eller tillhandahållande på annat sätt
- justering eller sammanförande
- begränsning
- radering eller förstöring

PERSONUPPGIFTSANSVARIG

Umeå universitet är personuppgiftsansvarig och har det yttersta ansvaret för all behandling av personuppgifter som sker inom ramen för verksamheten.

”En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer **ändamålen** och **medlen** för behandlingen av personuppgifter”

PERSONUPPGIFTSBITRÄDE

En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter **för den personuppgiftsansvariges räkning**.

Umeå universitet *anlitar* ofta personuppgiftsbiträden - ex vis molntjänstleverantörer, analysföretag, rekryteringsföretag

Umeå universitet *är* personuppgiftsbiträde i vissa fall – ex vis i den verksamhet som ITS bedriver.

- Personuppgiftsbiträdesavtal (PUBA) ska tecknas
- Endast universitetsdirektör är behörig att underteckna personuppgiftsbiträdesavtalen.
- - ett personuppgiftsbiträde får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige.

KÄNSLIGA PERSONUPPGIFTER
(SÄRSKILDA KATEGORIER AV PERSONUPPGIFTER)

- etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i en fackförening,
- hälsa,
- en persons sexualliv eller sexuella läggning,
- genetiska uppgifter,
- biometriska uppgifter som entydigt identifierar en person

KÄNSLIGA PERSONUPPGIFTER
(SÄRSKILDA KATEGORIER AV PERSONUPPGIFTER)

Huvudregeln är att det är förbjudet att behandla känsliga personuppgifter, men det finns en rad undantag.

Undantag ex vis:

- behandlingen krävs enligt lag,
- behandlingen är nödvändig för handläggningen av ett ärende,
- behandlingen är nödvändigt för att följa arkivföreskrifter
- behandlingen är nödvändig för forskning – dock krävs etikprövning.

PERSONUPPGIFTER SOM ÄR SÄRSKILT SKYDDSVÄRDA

- löneuppgifter
- uppgifter om lagöverträdelser
- värderande uppgifter, till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester
- information som rör någons privata sfär
- uppgifter om sociala förhållanden
- personnummer

PERSONNUMMER

Extra skyddsvärd uppgift.

Behandla bara personnummer om det är klart motiverat med hänsyn till

- ändamålet med behandlingen
- vikten av en säker identifiering
- något annat beaktansvärt skäl.

Personnummer bör exponeras så lite som möjligt.

Personnummer ska inte finnas på adressetiketter, i kuvertfönster eller i försändelser som sänds utan kuvert så att de är synliga för vem som helst.

GRUNDLÄGGANDE PRINCIPER

De grundläggande principerna ska genomsyra all behandling av personuppgifter.

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

LAGLIGHET, KORREKTHET OCH ÖPPENHET

All personuppgiftsbehandling måste

- Ha lagligt stöd – en rättslig grund
- Vara korrekt, rättvis, skälig, rimlig och proportionerlig
- De registrerade ska informeras om hur deras personuppgifter behandlas -lättillgängligt, begripligt, klart och tydligt

RÄTTSLIG GRUND FÖR BEHANDLING

- De rättsliga grunder vi normalt åberopar:
- **Allmänt intresse** (det ska finnas stöd i lag eller annan författning, kollektivavtal eller beslut som har meddelats med stöd av lag eller annan författning, ex vis högskolelagen)
- **Myndighetsutövning**
- **Rättslig förpliktelse**
- **Avtal**

SAMTYCKE

- Samtycke är också en rättslig grund.
- Endast undantagsvis ska Umeå universitet åberopa samtycke som rättlig grund.
- Samtycke – ex vis vid externa kontakter, användning av foton och filmer, studentarbeten

- *Samtycke kan inte användas som rättslig grund när det råder betydande ojämlikhet mellan den registrerade och personuppgiftsansvarige. En sådant ojämlikt förhållande kan vara särskilt vanligt mellan offentliga myndigheter och enskilda registrerade.*

REGISTRERADES RÄTTIGHETER

- Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas.
- Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige i samband med att uppgifterna samlas in (inte i efterhand med andra ord).
- Information (checklista för hur information ska lämnas finns på https://www.aurora.umu.se/globalassets/dokument/universitetsforvaltningen/universitetsledningens-kansli/juridik/checklista-information-till-registrerad-2018-10-17.pdf/

REGISTRERADES RÄTTIGHETER

- Om en registrerad kommer in med en **begäran om registerutdrag, att bli glömd, raderad** m.m. – se instruktion på Aurora https://www.aurora.umu.se/regler-och-riktlinjer/juridik/personuppgifter/
- Begäran från den registrerade om att få registerutdrag, att bli glömd, raderad - är **inte** samma sak som en begäran om utlämnande av allmän handling- den registrerade måste identifiera sig.

ÄNDAMÅLSBEGRÄNSNING

- Man får bara samla in personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål.
- Man måste därför ha klart för sig varför man ska behandla personuppgifterna redan när man börjar samla in dem.
- Ändamålen sätter ramarna för vad man får och inte får göra, till exempel vilka uppgifter man får behandla.

UPPGIFTSMINIMERING

- Man ska aldrig behandla fler personuppgifter än vad som behövs, och de personuppgifter som behandlas ska vara tydligt kopplade till ändamålet.
- Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov, för att de kan vara "bra att ha".

LAGRINGSMINIMERING

- personuppgifterna ska raderas eller avidentifieras när de inte längre behövs
- dataskyddsförordningen hindar inte myndigheter att arkivera handlingar som innehåller personuppgifter i det fall vi har en skyldighet enligt lag att arkivera handlingarna

Om vi är skyldiga att arkivera ska vi arkivera trots att handlingarna innehåller personuppgifter.

INTEGRITET OCH KONFIDENTIALITET

Personuppgifterna ska

- skyddas med lämpliga tekniska och organisatoriska åtgärder så att de inte blir åtkomliga för obehöriga, förstörs eller skadas
- Lämplig säkerhetsnivå
- Inte bara teknik, rutiner och instruktioner också

OFFENTLIGHETSPRINCIPEN

- Dataskyddsförordningen hindrar inte myndigheter att lämna ut allmänna handlingar enligt offentlighetsprincipen.
- GDPR-sekretess (sällan vid begäran om enstaka uppgifter eller journalistiska ändamål)

- om det kan antas att personuppgifterna kommer att behandlas i strid med GDPR, dataskyddslagen eller etikprövningslagen, *efter* att uppgifterna har lämnats ut till mottagaren, föreligger det sekretess för personuppgifterna

- Allmänna handlingar som innehåller personuppgifter bör i första hand lämnas ut i pappersform.

E-POST

- Innehåller alltid personuppgifter
- Används i vår verksamhet – med de lagliga grunder vi stödjer oss på där
- ”E-post ett särskilt utsatt färdmedel”. Tänk på säkerhet i färdvägarna och risken för spridning.
- Flytta epost till andra system/diarieför, ”arbeta” inte i e-posten
- Känsliga personuppgifter och sekretessbelagda uppgifter; undvik eller kryptera
- Integritetskänsliga uppgifter kan skickas i epost om det är fråga om enstaka uppgifter och vi kan säkerställa att mottagaren är den rätta.

E-POST

- Sprid inte i onödan, skicka inte adresser synligt utom organisationen
- Undvik att använda din e-post vid UmU för privat e-post eller e-post du skickar i inom ramen för någon annan roll du har, exempelvis som facklig företrädare.
- Informera de behandlade

https://www.aurora.umu.se/stod-och-service/blanketter-och-mallar/mallar-med-logotyp/

UMEÅ
UNIVERSITET

Namn Namnsson
Kommunikatör / Press officer
Kommunikationsenheten / Communications Office
Umeå universitet / Umeå University
SE-901 87 Umeå, Sweden
+46 (0)90 123 45 67 / +46 (0)72-123 4567
www.umu.se

När du skickar e-post till Umeå universitet innebär det att universitetet behandlar dina personuppgifter.
Läs mer här: umu.se/gdpr

E-mailing Umeå University means that we will process your personal data.
For more information, please read: umu.se/en/gdpr

PREFEKTERNAS/CHEFERNAS ANSVAR

Se till att verksamheten följer de regler och rutiner som universitetet har genom att skapa förutsättningar för en korrekt hantering.

Exempelvis:

- Se till att centralt beslutade rutiner och riktlinjer görs kända på institutionen/enheten
- Inom institutionens verksamhet ska behandling av personuppgifter genomlysas – behörighetsstyrning, teknisk säkerhet, lagring, gallrings- och arkiveringsrutiner mm.

ANSTÄLLDAS ANSVAR

- Samtliga anställda är inom ramen för sin anställning skyldiga att följa de regler och rutiner som arbetsgivaren ställer. Detta gäller även behandling av personuppgifter.

- För vissa anställda, som exv forskare med ansvar för ett forskningsprojekt som behandlar känsliga personuppgifter eller systemägare är detta ansvar än större.

PERSONUPPGIFTER I ANSTÄLLDAS DATORER

- Det finns troligen personuppgifter i era arbetsdatorer. Dataskyddsförordningen (GDPR) gäller för dessa uppgifter också.
- Så långt det går bör personuppgifter hanteras i gemensamma system med behörighetsstyrning.

ÖVERFÖRING AV PERSONUPPGIFTER TILL TREDJE LAND

Överföring av personuppgifter till tredje land är när personuppgifter blir tillgängliga för någon i ett land utanför EU/EES-området. Det är tillåtet i vissa fall, men reglerna är strikta. Kontakta pulo@umu.se för stöd om det är aktuellt.

Exempel

- När man anlitar ett personuppgiftbiträde i ett land utanför EU/EES.
- När man lagrar personuppgifter i en molntjänst som är baserad utanför EU/EES.
- När man lagrar personuppgifter, till exempel på en server, i ett land utanför EU/EES.

ANMÄLAN OM BEHANDLING

- Det finns krav på att den personuppgiftsansvarige ska föra register över var och hur personuppgiftsbehandling sker.
- Universitetet måste ha kontroll över de personuppgiftsbehandlingar vi är ansvariga och för och vi ska kunna visa att vi har kontroll. Gäller även när vi är personuppgiftsbiträde.

- Anmäl era personuppgiftsbehandlingar dataskyddsombudet om inte en generell anmälan finns.
- Avanmäl behandlingen när den upphör.

VILKA BEHANDLINGAR MÅSTE JAG ANMÄLA?

- Utbildning – central generell anmälan av förutsägbar behandling
- Administration/myndighetsärenden – central generell anmälan av förutsägbar behandling
- It-system – varje systemägare ansvarar för att anmälan sker
- Personuppgiftsbiträde – varje biträdesförhållande ska anmälas av ansvarig för avtalsförhållandet
- Forskning – varje forskningsprojekt där personuppgifter behandlas måste anmälas av ansvarig forskare.
- Studentarbeten – central generell anmälan dock måste man på institutionsnivå ha koll på studenternas personuppgiftsbehandlingar

HUR GÖR MAN FÖR ATT ANMÄLA?

- UmU använder sig av Draft-It som registersystem.
- Skriv ett meddelande till dataskyddsombudet på pulo@umu.se och beskriv kortfattat vilken kategori av behandling det är fråga om.
- Du får ett svar med en länk till registersystemet Draft-it och kan logga in och göra din anmälan.

SÄKERHET I SAMBAND MED PERSONUPPGIFTSBEHANDLINGAR

UMEÅ UNIVERSITET

INBYGGT DATASKYDD OCH DATASKYDD SOM STANDARD

- Dataskyddsförordningen ställer krav på att vi för våra IT-system ska vidta lämpliga tekniska åtgärder.
- Inbyggt dataskydd (privacy by design) som innebär att man redan vid utformningen av IT-system tar hänsyn till integritetsskyddsreglerna
- Dataskydd som standard (privacy by default) innebär att Umu ska se till att personuppgifter i standardfallet inte behandlas i onödan genom inställningar och liknande i systemen.
- *Detta innebär att systemägare som ska införskaffa ett nytt system behöver ta kontakt med pulo@umu.se redan i förberedelsestadiet av inför upphandling av systemet så att dessa krav kan ingå i skallkravet i upphandlingen.*

UMEÅ UNIVERSITET

LAGRINGSLÖSNINGAR OCH SAMARBETSYTOR

UMEÅ UNIVERSITET

VAR LAGRAR NI DOKUMENT?

- Gemensamma samarbetsytor och centrala system
  - Undvik att sprida informationen genom att ta ut informationen från systemet!
- Filytor – personliga och gemensamma
- Använd godkända molntjänster!
  - Var lagras informationen? Vem äger informationen? Går det att radera uppgifterna?

Tänk på att exempelvis Doodle eller en PDF-konverterare är en molntjänst!

UMEÅ UNIVERSITET

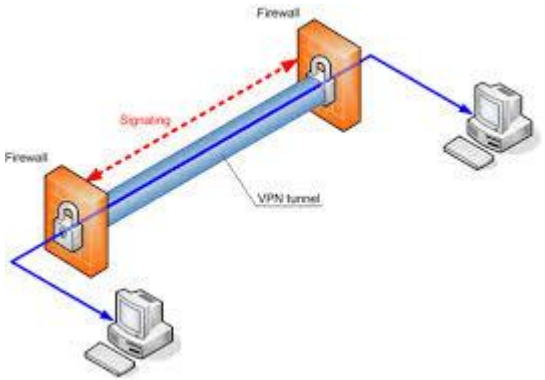
HUR KAN EN SÄKER ARBETSPLATS SE UT?

- Fördelar med sammanhållen hantering av datorer
  - Inventering
  - Automatiska uppdateringar
  - Antivirus
  - Paketering av program i SoftwareCenter
  - Kryptering av hårddisk
  - Backup

ANVÄND VPN

Ger säkrare förbindelse – skyddad kommunikations-kanal.

Underlättar för dig att få åtkomst till system vid Umu.



INCIDENTRAPPORTERING

- Personuppgiftsincident är en säkerhetsincident som kan innebära risker för den registrerade – uppgifterna förstörs eller kommer i orätta händer vilket kan leda till ID-stöld, bedrägeri, ekonomisk förlust, sekretessbrott m.m.
- Misstänker du att det har skett en personuppgiftsincident vänder du dig till IRT (Incident Response Team).
- IRT når du på abuse@umu.se.
- Under vissa förutsättningar kommer incidenten att anmälas till Datainspektionen.

MER INFORMATION

- Läs mer på Aurora

Regler och riktlinjer/ Juridik/ Personuppgifter

- Läs mer på Datainspektionens hemsida

www.datainspektionen.se