UPPSALA UNIVERSITET

Workshop inför dataskyddsförordningen, GDPR

Klassificera information i verksamheten

Identifiera system och andra ytor där personuppgifter behandlas.

Inventera och åtgärda brister i säkerhetsskyddet i de system som behandlar personuppgifter.

Dataskyddsförordningen

General Data Protection Regulation (GDPR)

Träder i kraft **25 maj 2018** och ersätter lokal lagstiftning som exempelvis Personuppgiftlagen, PuL

Syfte att:

– Stärka integritetsskyddet

– Möta teknikens förändringar

– Underlätta handel inom EU

Tillsynsmyndighet i Sverige är *Datainspektionen* (byter namn till Integritetsskyddsmyndigheten under 2018):

Information om Dataskyddsförordningen, GDPR:
https://www.datainspektionen.se/dataskyddsreformen

UPPSALA UNIVERSITET

Dataskyddsförordningen

För den enskilde medborgaren

Rättigheterna stärks vid hantering av personuppgifter:

Rätten att bli ”glömd” i vissa situationer

- Direktreklam eller liknande.
- Ej korrekta eller irrelevanta sökning exempelvis i Google.
- Uppgifter får dock sparas om det är legitimt.

Dataportabilitet

- Flytta uppgifter från sociala nätverk.
- Byte av leverantör.

UPPSALA UNIVERSITET

Dataskyddsförordningen

För företag, myndigheter organisationer

Obligatorisk rapportering vid intrång eller förlust av personuppgift inom 72 timmar).

Konsekvensanalys vid behandling av känsliga personuppgifter som exempelvis genetiska eller biometriska data.

Sanktionsavgifter (viten) vid utebliven efterlevnad av GDPR.

UPPSALA UNIVERSITET

Praktisk tillämpning av principerna

- Bestäm **ändamålet** och håll dig till det
  - Samla endast in uppgifter som behövs
  - Samla inte in fler uppgifter än nödvändigt
  - Använd inte uppgifter till ett annat oförenligt ändamål
  - Radera uppgifterna när de inte längre behövs för ändamålet
- Identifiera **rättslig grund** för behandlingen
- **Informera** på ett öppet och ärligt sätt
- Se till att **uppgifterna är korrekta och uppdaterade**
- **Skydda** insamlade uppgifter
- Se till att du **kan visa** att du gör rätt
  - Dokumentera
  - Förteckning över behandlingar
  - Rutiner och organisation

Källa: Datainspektionen 2018-03-20

UPPSALA UNIVERSITET

Dataskyddsförordningen

De största skillnaderna som GDPR kommer att resultera i, jämfört med dagens PUL (dataskyddsdirektivet) är främst:

- Mer och lättförståelig information ska ges till den enskilde personuppgifterna samlas in ifrån. Den enskilde ska kunna bli glömd och få information rättad och raderad.
- Grundas behandlingen på samtycke ska man kunna visa och bevisa att samtycket har lämnats.
- Att den personuppgiftsansvariges (Uppsala universitets) ansvar har förtydligats och en sanktionsavgift införs om denne inte följer förordningen.
- Personuppgiftsombudet blir istället ett Dataskyddsombud med en starkare ställning.
- En skyldighet att rapportera personuppgiftsincidenter inom 72 timmar till datainspektionen.
- Tydligare krav på att skydda uppgifterna med säkerhetsåtgärder.
- Hårdare regler vid tredjelandsöverföring med större krav på ansvar.

Dataskyddsförordningen
- Anmälan om personuppgiftsbehandling

Två nya e-blanketter kommer att publiceras för att kunna anmäla register över personuppgiftsbehandlingar (registerförteckning).

1. När **UU är personuppgiftsansvarig** (när vi behandlar ”våra egna” personuppgifter.

2. När **UU är personuppgiftsbiträde** (när vi behandlar personuppgifter för en annans räkning).

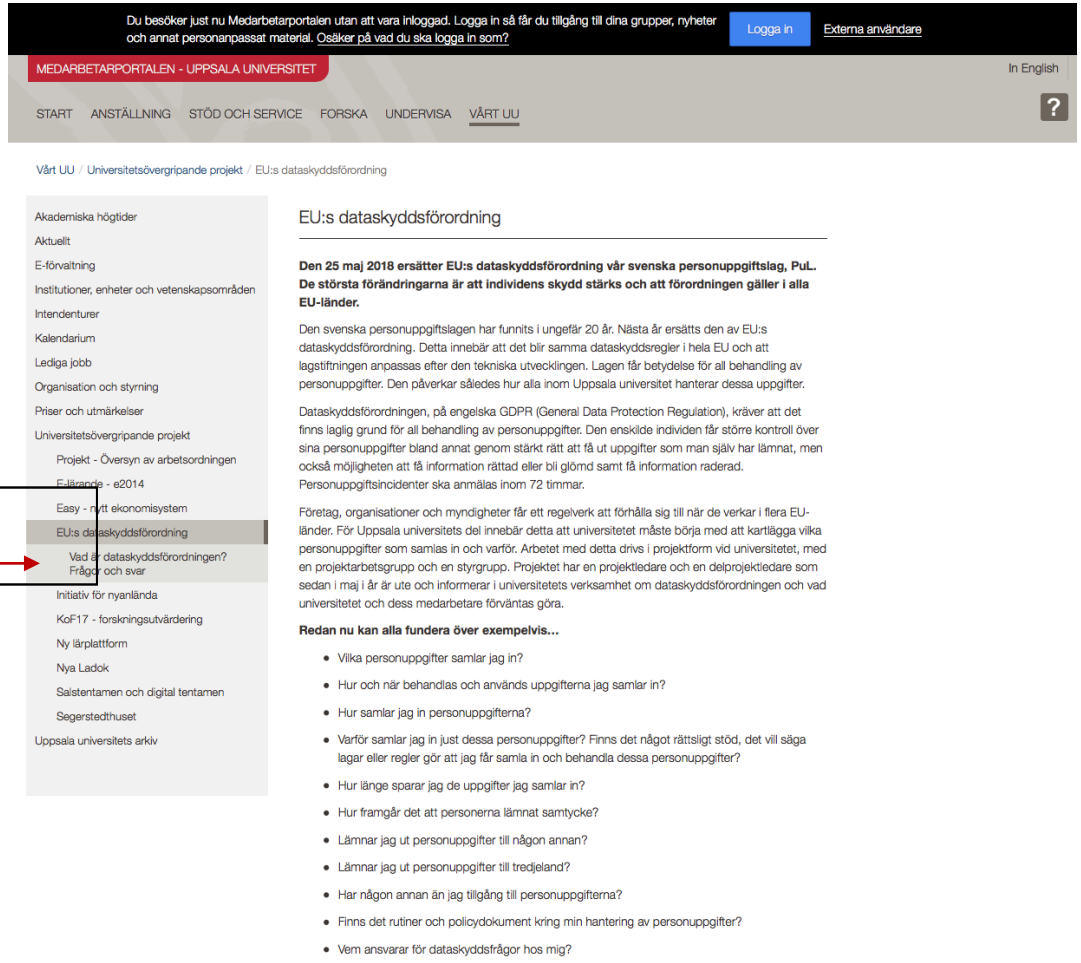
*Syftet är att ha kontroll på **vilka** behandlingar vi har och **var** vi har dem.*

Information om Dataskyddsförordningen

Medarbetarportalen,

Vårt UU/ Universitetsövergripande projekt /EU:s dataskyddsförordning

Vad är dataskyddsförordningen?
Frågor och svar



Anpassning till Dataskyddsförordningen

Avsnitt i projektets handlingsplan

- Inventera, uppdatera och beskriv policys, processer och annan dokumentation som är av intresse i behandlingen av personuppgifter.
- Uppdatera avtal.
- Fortsätta arbetet med att medvetandegöra efterlevnaden av dataskyddsförordningen.
- Den registrerades rättigheter att få tillgång till sina personuppgifter samt information till de registrerade.
- Upprätta registerförteckning avseende Uppsala universitets system och register som innehåller personuppgifter.
- Utred rättsligt stöd.
- **Tillsätt Dataskyddsombud**.
- Hantering av samtycke.
- Rätt att bli bortglömd.
- Dataöverföring (portabilitet).
- Ta fram rutin för hantering av personuppgiftsincident och tydliggör ansvar och roller.
- Säkerhet avseende insamling och hantering av personuppgifter.
- Inbyggt dataskydd (privacy by design).
- Identifiera system och andra ytor där personuppgifter behandlas.
- Definiera ”best practice”-skyddsåtgärder för system som behandlar personuppgifter.
- Inventera och åtgärda brister i säkerhetsskyddet i de system som behandlar personuppgifter.
- Utvärdera och följ upp.

Återkommande fråga till projektgruppen om ”rätten att bli glömd”

Rätten att bli glömd (enligt Datainspektionen)

- finns under vissa förutsättningar, men är inte definitiv.
- är förknippad med stora begränsningar när det gäller information som hanteras vid en myndighet.
- finns ett legitimt skäl att behålla uppgifterna kan detta alltså ske trots att personen ifråga velat ha dem raderade. Exempelvis för att utföra en uppgift av allmänt intresse eller som ett led i myndighetsutövning.

UPPSALA
UNIVERSITET

Dataskyddsombudet…

…och lite om dataskyddsförordningen

Jacob Håkansson

UPPSALA UNIVERSITET

Datainspektionen om dataskyddsombudet

Dataskyddsförordningen om dataskyddsombud

Artikel 37: Utnämning av dataskyddsombudet

1. Den personuppgiftsansvarige och personuppgiftsbiträdet ska under alla omständigheter utnämna ett dataskyddsombud om

a) behandlingen genomförs av en myndighet eller ett offentligt organ, förutom när detta sker som en del av domstolarnas dömande verksamhet,

Datainspektionens kommentar

Myndigheter och offentliga organ måste alltså ha ett dataskyddsombud oavsett vilka uppgifter de behandlar. Det gäller inte för andra organisationer. De måste ha ett dataskyddsombud bara om de faller inom kategorierna b och c nedan.

Men även privata organisationer kan bedriva offentlig verksamhet och myndighetsutövning, till exempel inom kollektivtrafik, vatten- och energiförsörjning, väginfrastruktur, radio och tv i allmänhetens tjänst, allmännyttiga bostäder eller disciplinorgan för reglerade yrken. För de registrerade är det ungefär samma sak om deras personuppgifter behandlas av en myndighet eller ett offentligt organ. Ett dataskyddsombud kan då ge de registrerade skydd och trygghet.

Datainspektionen rekommenderar därför att privata organisationer som bedriver offentlig verksamhet och myndighetsutövning utnämner ett dataskyddsombud.

b) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling som, på grund av sin karaktär, sin omfattning och/eller sina ändamål, kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning, eller

Datainspektionens kommentar

"Kärnverksamhet" är den nödvändiga centrala verksamhet som en organisation utför för att uppfylla sitt uppdrag och sina mål.

Exempel: Ett säkerhetsföretag kameraövervakar flera köpcentrum. Deras kärnverksamhet är säkerhet, men de måste filma personer, vilket innebär att de behandlar personuppgifter i stor omfattning. Personuppgiftsbehandling är alltså en del av deras kärnverksamhet.

Men alla organisationer behandlar personuppgifter i stödjande verksamheter, till exempel för att betala ut lön, eller i samband med it-stöd. Det är exempel på nödvändiga stödfunktioner för organisationens kärnverksamhet eller huvudsakliga verksamhet. Även om sådana verksamheter är nödvändiga eller centrala, så är de inte kärnverksamhet utan kompletterande funktioner. Icke-offentliga organ som bara behandlar personuppgifter på det sättet behöver alltså inte något dataskyddsombud.

"Regelbunden" betyder

•pågående övervakning eller övervakning som sker i vissa intervall eller under en viss period
•återkommande eller upprepad övervakning vid fasta tidpunkter
•ständig eller periodisk övervakning.

"Systematisk" är övervakning som

•sker enligt ett system
•är på förhand arrangerad, organiserad eller metodisk övervakning
•sker enligt en allmän plan för insamling av personuppgifter
•utförs som ett led i en strategi.

"Regelbunden och systematisk övervakning av de registrerade" omfattar alltså till exempel

•alla former av spårning och profilering på internet
•drift av ett telekommunikationsnät
•tillhandahållande av telekommunikationstjänster
•datadriven marknadsföring
•profilering eller poängsättning för riskbedömningar till exempel för bedömning av kreditvärdighet, fastställande av försäkringspremier
•förebyggande av bedrägeri, upptäckt av penningtvätt
•positionsspårning, till exempel genom mobilappar
•lojalitetsprogram
•beteendestyrd annonsering
•övervakning av välbefinnande, träning och hälsa via exempelvis aktivitetsarmband

UPPSALA UNIVERSITET

Dataskyddsförordningen och dataskyddslag

Regeringens proposition
2017/18:105

Ny dataskyddslag

Prop.
2017/18:105

Regeringen överlämnar denna proposition till riksdagen.

Stockholm den 15 februari 2018

Stefan Löfven

Morgan Johansson
(Justitiedepartementet)

Propositionens huvudsakliga innehåll

Regeringen föreslår att personuppgiftslagen upphävs och att en ny lag med kompletterande bestämmelser till EU:s dataskyddsförordning införs. Vidare föreslås att vissa bestämmelser i offentlighets- och sekretesslagen ändras.

Den föreslagna lagen innehåller bl.a. bestämmelser om att dataskyddsförordningen med vissa undantag ska gälla även utanför sitt egentliga tillämpningsområde, t.ex. i verksamhet som rör nationell säkerhet. Lagen ska dock vara subsidiär i förhållande till annan lag eller förordning, vilket möjliggör avvikande bestämmelser i s.k. registerförfattningar. Lagförslaget förtydligar under vilka förutsättningar personuppgifter får behandlas med stöd av dataskyddsförordningen. Regeringen föreslår bl.a. att ett barn som är minst 13 år ska kunna samtycka till behandling av personuppgifter i samband med användning av informationssamhällets tjänster, t.ex. sociala medier. Vidare föreslås att sanktionsavgifter ska kunna tas ut även då en myndighet bryter mot dataskyddsförordningen. Förslaget till ny lag innehåller också vissa bestämmelser om begränsning av de registrerades rättigheter samt om skadestånd och överklagande av bl.a. tillsynsmyndighetens beslut.

Slutligen anges att dataskyddsförordningen och den nya lagen inte ska tillämpas i den utsträckning det strider mot tryckfrihetsförordningen eller yttrandefrihetsgrundlagen.

Lagändringarna föreslås träda i kraft den 25 maj 2018.

1

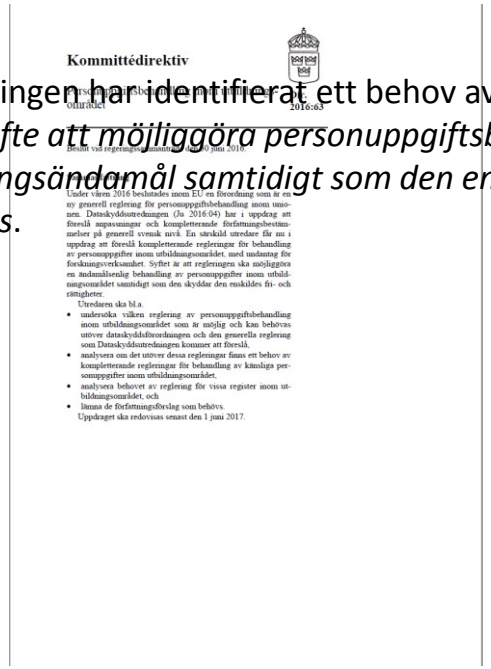
Dataskyddslagen = Nationella kompletteringar till dataskyddsförordningen

- Utredningen föreslår en ny dataskyddslag.
- Målsättning: Bevara så mycket som möjligt av tidigare bestämmelser – en del personuppgiftsbehandling kommer därför att bli densamma.
- Preciserar vad som skall gälla för svenska förhållanden.

UPPSALA UNIVERSITET

Direktiv för utredning av personuppgiftsbehandling (PuB) inom forskning och utbildning

PuB inom utbildningsområdet



Kommittédirektiv

Dir. 2016:63

Beslut vid regeringssammanträde den 9 juni 2016

Sammanfattning

Under våren 2016 beslutades inom EU en förordning som är en ny generell reglering för personuppgiftsbehandling inom unionen. Dataskyddsutredningen (Ju 2016:04) har i uppdrag att föreslå anpassningar och kompletterande författningsbestämmelser på generell svensk nivå. En särskild utredare får nu i uppdrag att föreslå kompletterande regleringar för behandling av personuppgifter inom utbildningsområdet, med undantag för forskningsverksamhet. Syftet är att regleringen ska möjliggöra en ändamålsenlig behandling av personuppgifter inom utbildningsområdet samtidigt som den skyddar den enskildes fri- och rättigheter.

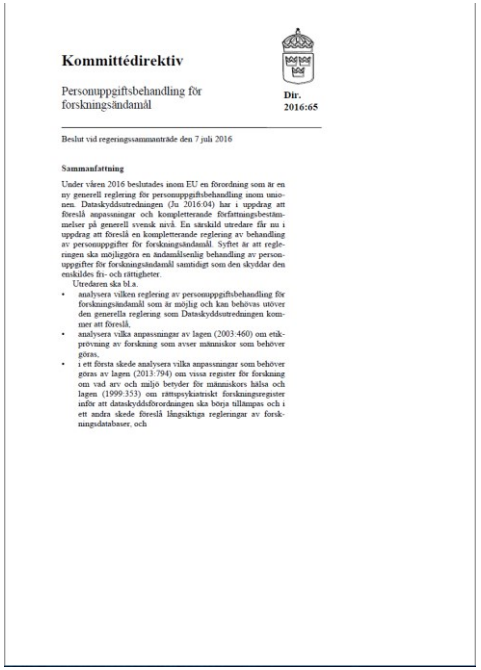
Utredaren ska bl.a.

- undersöka vilken reglering av personuppgiftsbehandling inom utbildningsområdet som är möjlig och kan behövas utöver dataskyddsförordningen och den generella regleringen som Dataskyddsutredningen kommer att föreslå,
- analysera om det utöver dessa regleringar finns ett behov av kompletterande regleringar för behandling av känsliga personuppgifter inom utbildningsområdet,
- analysera behovet av reglering för vissa register inom utbildningsområdet, och
- lämna de författningsförslag som behövs.

Uppdraget ska redovisas senast den 1 juni 2017.

Utredningen har identifierat ett behov av att införa en forskningsdatalag med *syfte att möjliggöra personuppgiftsbehandling för forskningsändamål samtidigt som den enskildes fri- och rättigheter skyddas*.

PuB för forskningsändamål



Kommittédirektiv

Personuppgiftsbehandling för forskningsändamål

Dir. 2016:65

Beslut vid regeringssammanträde den 7 juli 2016

Sammanfattning

Under våren 2016 beslutades inom EU en förordning som är en ny generell reglering för personuppgiftsbehandling inom unionen. Dataskyddsutredningen (Ju 2016:04) har i uppdrag att föreslå anpassningar och kompletterande författningsbestämmelser på generell svensk nivå. En särskild utredare får nu i uppdrag att föreslå en kompletterande reglering av behandling av personuppgifter för forskningsändamål. Syftet är att regleringen ska möjliggöra en ändamålsenlig behandling av personuppgifter för forskningsändamål samtidigt som den skyddar den enskildes fri- och rättigheter.

Utredaren ska bl.a.

- analysera vilken reglering av personuppgiftsbehandling för forskningsändamål som är möjlig och kan behövas utöver den generella regleringen som Dataskyddsutredningen kommer att föreslå,
- analysera vilka anpassningar av lagen (2003:460) om etikprövning av forskning som avser människor som behöver göras,
- i ett första skede analysera vilka anpassningar som behöver göras av lagen (2013:794) om vissa register för forskning om vad arv och miljö betyder för människors hälsa och lagen (1999:353) om rättspsykiatriskt forskningsregister inför att dataskyddsförordningen ska börja tillämpas och i ett andra skede föreslå lämpliga regleringar av forskningsdatabaser, och

UPPSALA
UNIVERSITET

Lämpliga åtgärder för integritet och konfidentialitet?

Till den generella regleringen hör även allmänna skyldigheter för den ***personuppgiftsansvarige att genomföra lämpliga tekniska och organisatoriska åtgärder för att kunna säkerställa och visa att behandlingen utförs i enlighet med dataskyddsförordningen*** *(artikel 24), samt krav på att säkerställa en lämplig säkerhetsnivå (artikel 32).*

UPPSALA UNIVERSITET

Peter Eriksson
Bostads- och digitaliseringsminister
Näringsdepartementet

Regeringskansliet

Lyssna | English website | Lättläst | Teckenspråk | Other languages | Prenumerera via e-post | Kontakt

Jobba hos oss | Press | Sverige i EU | UD:s reseinformation

Sök på regeringen.se — Sök

Sveriges regering
Statsråden och departementen

Regeringens politik
Detta görs inom olika områden

Så styrs Sverige
Om regeringen, Regeringskansliet och EU

Datainspektionen blir Integritetsskyddsmyndigheten

Regeringen tillför Datainspektionen 30 miljoner för att stärka arbetet med den personliga integriteten. Myndigheten kommer byta namn till Integritetsskyddsmyndigheten och ges i uppdrag att agera stödjande och rådgivande för att tjänster som ökar medborgarnas livskvalitet kan fortsätta utvecklas och användas samtidigt som den personliga integriteten värnas.

Den allt snabbare digitaliseringen av samhället ställer höga krav på att enskildas rättigheter och personliga integritet kan värnas. Samtidigt måste data kunna användas på ett sätt som återspeglar det moderna samhällets behov. Det måste finnas förutsättningar för att utveckla och använda tjänster som ökar medborgarnas livskvalitet och näringslivets konkurrenskraft. Sverige behöver kunna hantera och möjliggöra den utveckling som sker av avancerad informationsteknik, som exempelvis artificiell intelligens (AI) och algoritmer som behandlar stora datamängder.

– Med dessa förändringar skapar vi förutsättningar för att utveckla och använda nya tjänster samtidigt som den personliga integriteten värnas, säger digitaliseringsminister Peter Eriksson.

- Datainspektionens blir en central tillsynsmyndighet på området och byter namn till Integritetsskyddsmyndigheten.
- Myndighetens uppdrag kommer att ändras så att dess stödjande och rådgivande roll blir tydligare.
- Myndigheten tillförs 30 miljoner kronor extra från och med 2018
- Myndigheten får också i uppdrag att löpande följa utvecklingen inom integritetsskydd
- EU:s dataskyddsreform som börjar gälla under 2018 är den största integritetsstärkande reformen på länge.

UPPSALA UNIVERSITET

Problem med personuppgifter?

- **Ändamålsbegränsning:**
- Bara behandling med hänsyn till särskilda, uttryckligt angivna och berättigade ändamål.
- Inte senare behandlas på sätt som är oförenliga med detta ändamål.

DIGITAL

Facebook riskerar miljardbot i Belgien | Ta chansen att vinna ett företag – med din idé SPONSRAT AV TELE2 | Dyster försäljningsprognos från Rovio får aktien att rasa | Stillfront mer än fördubblar omsättningen | Podd: "Alla vill inte jobba på Klarna"

Av DI DIGITAL | måndag 19 februari 2018 kl. 15:00 | digital@di.se | @didigital_se

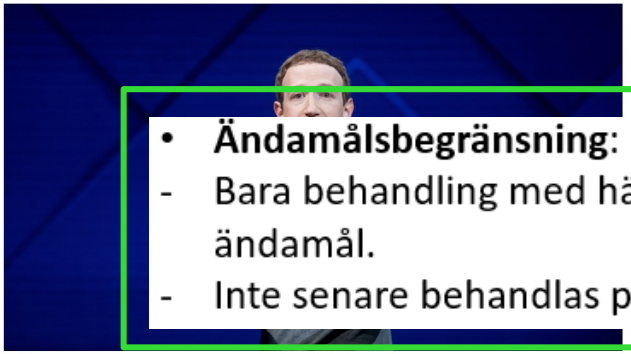


Foto: Noah Berger

Facebook åker på ett nytt bakslag i Belgien.

FACEBOOK
TWITTER
LINKEDIN
E-POST
ÖKA TEXTSTORLEK

Facebook riskerar böter på upp emot 100 miljoner euro, motsvarande 991 miljoner kronor, efter att en domstol i Belgien återigen dömt att företaget brutit mot privatlagar när man spårade icke-användare utanför sociala plattformen. Det rapporterar Techcrunch.

Läs mer: Facebook får böter i Spanien för att ha brutit mot integritetsregler

Facebook uppges med användning av cookies och plug-ins ha spårat icke-användare på andra ställen runt på Internet. Bakgrunden till detta var att kunna samla in data om dem och därefter erbjuda dem riktad reklam.

På di.se använder vi cookies för att din läsarupplevelse ska bli så bra som möjligt. Genom att fortsätta använda vår webbplats accepterar du att cookies används. Läs mer om cookies här.

Jag förstår

Facebook får böter i Spanien för att ha brutit mot integritetsregler

Av DI DIGITAL | måndag 11 september 2017 kl. 13:58 | digital@di.se | @didigital_se

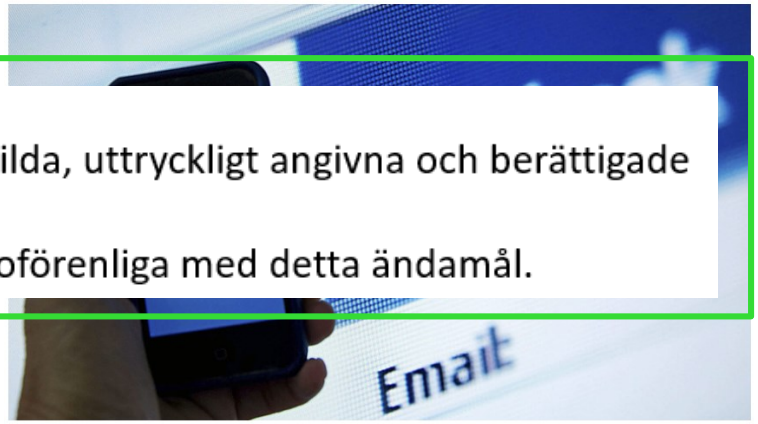


Foto: KAREN BLEIER

Nu tvingas nätverksjätten Facebook betala böter i Spanien.

FACEBOOK
TWITTER
LINKEDIN

Facebook tvingas böta i Spanien. Myndigheter i landet har slagit fast att företaget sammanställt personliga uppgifter om sina användare, som kunnat användas av annonsörer, utan att användarna har gett sitt "fulla medgivande" eller informerats om detta.

Facebook ska böta 1,2 miljoner euro, motsvarande cirka 11,5 miljoner

UPPSALA UNIVERSITET

Personuppgifter och känsliga personuppgifter

Personuppgifter:

- varje upplysning som avser en identifierad eller identifierbar fysisk person, t.ex.
- namn
- ett identifikationsnummer
- en lokaliseringsuppgift eller onlineidentifikatorer
- eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Känsliga personuppgifter:

1. ras eller etniskt ursprung
2. politiska åsikter
3. religiös eller filosofisk övertygelse
4. medlemskap i en fackförening
5. hälsa
6. en persons sexualliv eller sexuella läggning
7. genetiska uppgifter och
8. biometriska uppgifter som entydigt identifierar en person.

UPPSALA UNIVERSITET

Att behandla personuppgifter efter den 25 maj 2018?

Man får behandla personuppgifter, men

- det måste finnas ett klart angivet **ändamål**, och
- behandlingen måste vara **nödvändig** för ändamålet, och
- så skall det finnas en **laglig grund** för behandlingen som skall,
- **skyddas** av tekniska och andra åtgärder.

UPPSALA UNIVERSITET

Laglig grund?

- **Samtycke** = frivilligt och uttalat.
- **Avtal** = för att fullgöra ett avtal eller på begäran av den registrerade.
- **Rättslig förpliktelse** = Om lag tvingar till behandling av personuppgifter.
- **Skydd för grundläggande intresse** = Om någons grundläggande intresse kräver behandlingen.
- **Uppgift av allmänt intresse och myndighetsutövning** = Om myndighetens arbete kräver behandlingen.
- **Intresseavvägning** = Om berättigade intressen för behandling väger tyngre än skyddet av den enskildes rättigheter.

UPPSALA UNIVERSITET

Dataskyddsombudets uppgifter

Vad skall uträttas:

1. Samla in information om hur organisationen behandlar personuppgifter.
2. Kontrollera att organisationen följer bestämmelser och interna styrdokument.
3. Informera och ge råd inom organisationen.
4. Dataskyddsombudet ska också ge råd om konsekvensbedömningar.
5. Vara kontaktperson för Datainspektionen.
6. Vara kontaktperson för registrerade och för personal inom organisationen.
7. Samarbeta med Datainspektionen, till exempel vid inspektioner.

Ansvaret för behandlingen av personuppgifter vid UU?

Dataskyddsombudet har inget eget ansvar för att organisationen följer dataskyddsförordningen. √

Personuppgiftsansvariga får heller inte bestraffa dataskyddsombudet för att ha utfört sina arbetsuppgifter.

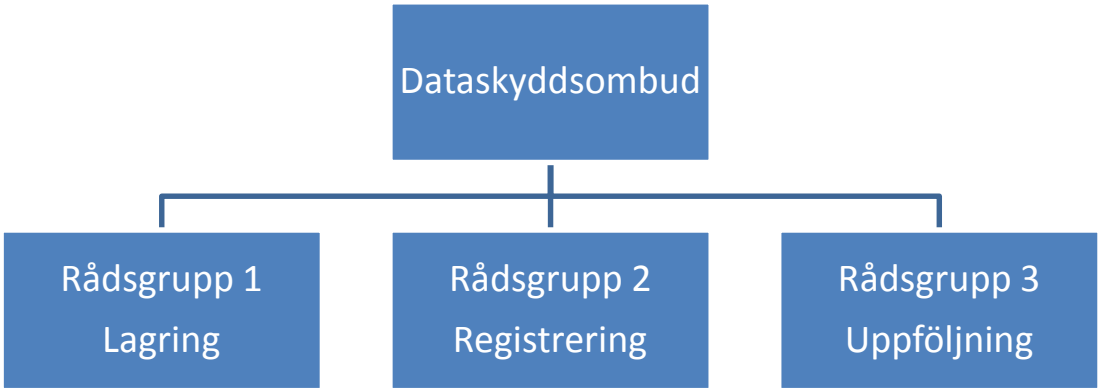
√

Ansvaret för personuppgiftsbehandlingen ligger alltid hos den personuppgiftsansvariga eller hos personuppgiftsbiträdet. √

UPPSALA UNIVERSITET

Dataskyddsgrupper?

UPPSALA UNIVERSITET



Info-säkerhet - Juridik - IT - **Verksamhetsanknytning** - Omvärldsbevakning

UPPSALA UNIVERSITET

Automatiserade rutiner för dataskyddsfrågor

En liten del i ett stort sammanhang

som lägger grunden för säker informationshantering

Medvetandegöra efterlevnaden

registrerades rättigheter

Hantering av samtycke

Upprätta registerförteckning

Utred rättsligt stöd

Policys, processer

Rätt att bli bortglömd

Inbyggt dataskydd

Uppdatera avtal

Informationsklassificering

m.m.

Fokus för denna workshop

- Vilken information?
- Hantering var, hur och vilka roller?
- Ett första steg i att utreda om informationen omges av ett tillräckligt starkt skydd?

UPPSALA UNIVERSITET

Ett möte mellan universitetets informationssäkerhetarbete och arbetet med anpassningar inför dataskyddsförordningens införande

Från GDPR-projektetets aktivitetsplan

- Identifiera system och andra ytor där personuppgifter behandlas.
- Definiera ”best practice”-skyddsåtgärder för system som behandlar personuppgifter.
- Inventera och åtgärda brister i säkerhetsskyddet i de system som behandlar personuppgifter.

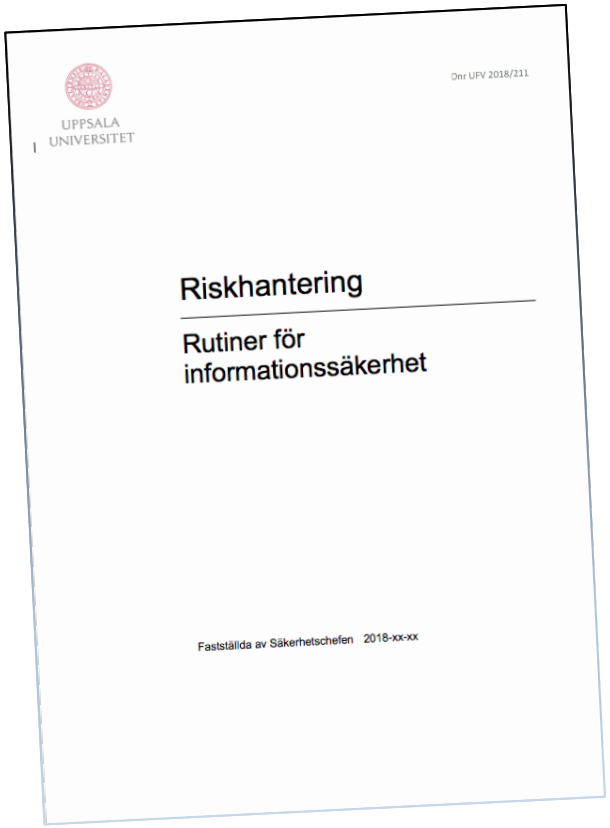
MSB:s föreskrifter MSBFS 2016:1

9 § I syfte att hantera hot och risker som rör informationssäkerheten i verksamheten ska myndigheten med stöd av modeller som myndigheten beslutar

1. klassa information med utgångspunkt i konfidentialitet, riktighet och tillgänglighet i olika nivåer utifrån vilka konsekvenser som kan uppstå av ett bristande skydd,
2. identifiera, analysera och bedöma hot och risker för verksamhetens information, system och tjänster …

UPPSALA UNIVERSITET

Stöddokument
- Riskhantering,uppdaterad riktlinje


UPPSALA UNIVERSITET

Dnr UFV 2018/211

Riskhantering

Rutiner för informationssäkerhet

Fastställda av Säkerhetschefen 2018-xx-xx

- *Riskhantering, rutiner för informationssäkerhet, UFV 2018/211*
- Stöd vid genomförande av informationsklassificering och kravanalyser för bedömning och behandling av säkerhetsrisker
- Praktiskt och verksamhetsanpassat stöd för kontinuerlig riskhantering av universitetets informationsresurser

UPPSALA UNIVERSITET

Riskhanteringsprocessen

1. **Avgränsning.** *Vilka system*, systemdelar, gränssnitt etc. ska ingå i analysen? (Vad ska ingå i analysen?)

2. **Informationsklassificering med utgångspunkt från en referenstabell**. Vilken information hanteras av systemen/et och hur känslig är den med avseende på konfidentialitet, riktighet och tillgänglighet? (klasser: representeras av siffror 0-3).

3. **Kravanalys.** Säkerhetsmässiga krav mappas mot resultatet från genomförd riskanalys (nulägesbedömning). Planering av åtgärder för identifierade GAP.

4. ***Riskanalys.*** *Kan genomföras som ett kompletterande moment.*

5. **Åtgärdsplan för säkerhetsförbättringar.**

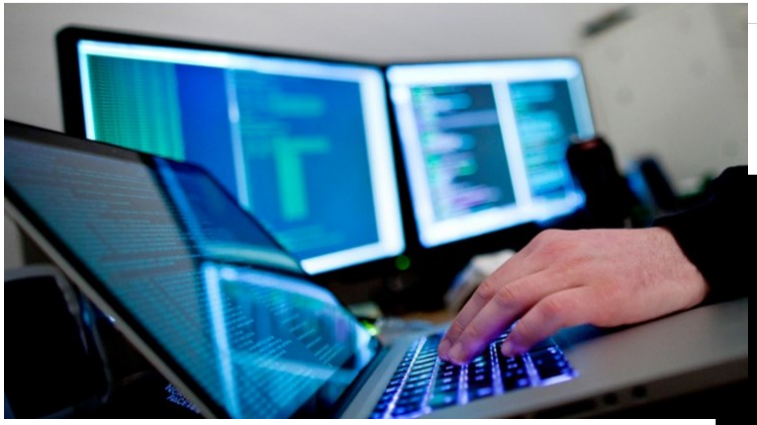
UPPSALA UNIVERSITET

Varför? Inte bara för att slippa betala vite …

Stora brister i IT-säkerhet hos svenska myndigheter

Publicerat torsdag 4 september 2014 kl 05.30

"Myndigheterna måste ta sitt ansvar"
(2:11 min)

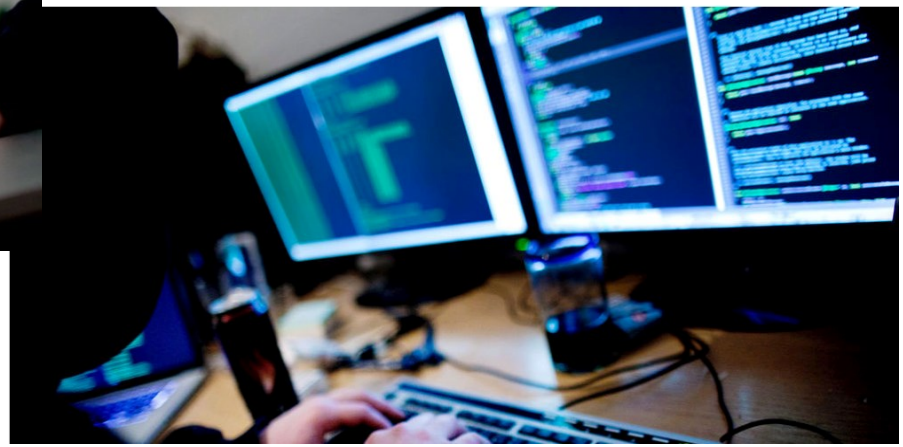


Allvarliga brister funna i Riksbankens it-säkerhet

PREMIUM SvD AVSLÖJAR | Känslig information som riskerar att hamna i orätta händer, allvarliga incidentrapporter som slarvas bort, dåligt krypterad kommunikation och slarv i hantering av hemlig data. Riksbankens informationssäkerhet har ett flertal anmärkningsvärda brister.

Sverige

Flera svenska myndigheter kan ha hackats



It-skandalen inom Transportstyrelsen

It-intrången upptäcktes aldrig

Lyssna

Sigtuna kommuns it-system innehåller flera brister. När konsulter skulle testa it-avdelningens agerande vid intrång i kommunens it-system upptäcktes de aldrig.

Lars Johansson

12:17 | 2018-02-19

UPPSALA UNIVERSITET

Informationsklassificering utgör grunden

Klasser (skyddsnivåer/konsekvensvärden):
Tidigare använda: Bas, Hög och Särskilda krav.
I den nya modellen: **0, 1, 2 eller 3**.

Bedöms för var och en av nedanstående säkerhetsaspekter:

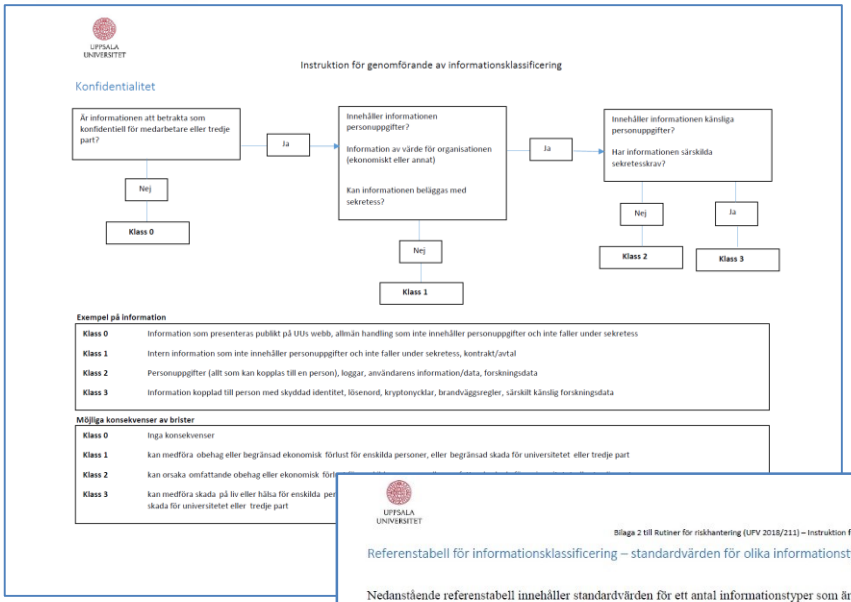
Konfidentialitet:	Informationen ska inte göras tillgänglig eller avslöjas för obehöriga personer, system eller processer.
Riktighet:	Informationen ska inte förändras eller förstöras, varken obehörigen, av misstag eller pga. funktionsstörningar.
Tillgänglighet:	Informationen ska vara åtkomlig och användbar på förväntat sätt och inom önskad tid.

Informationen får ett KRT-värde, exempelvis 322

UPPSALA UNIVERSITET

Rutiner för riskhantering – bilaga 2

En hjälp att hitta rätt i klassningsarbetet



UPPSALA UNIVERSITET

Instruktion för genomförande av informationsklassificering

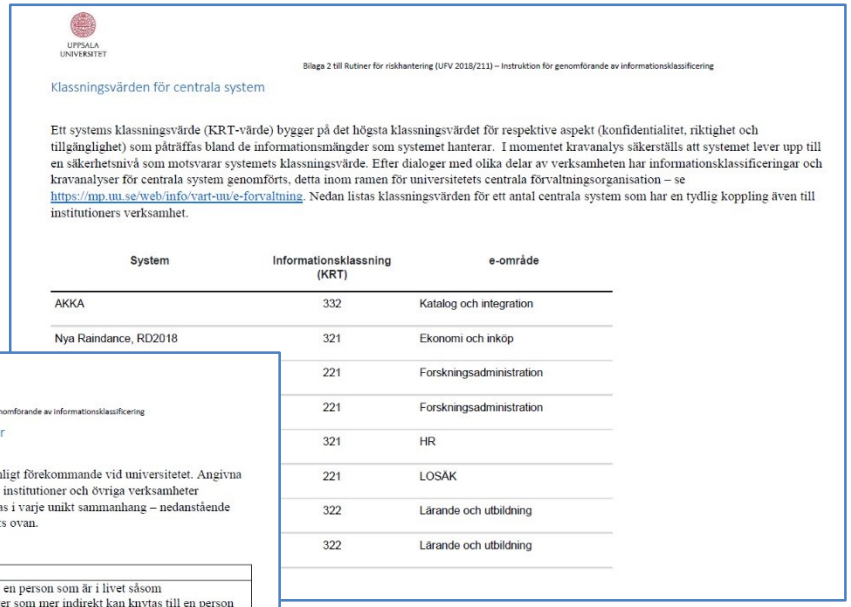
Konfidentialitet

Exempel på information

Klass 0	Information som presenteras publikt på UUs webb, allmän handling som inte innehåller personuppgifter och inte faller under sekretess
Klass 1	Intern information som inte innehåller personuppgifter och inte faller under sekretess, kontrakt/avtal
Klass 2	Personuppgifter (allt som kan kopplas till en person), loggar, användarens information/data, forskningsdata
Klass 3	Information kopplad till person med skyddad identitet, lösenord, kryptonycklar, brandväggsregler, särskilt känslig forskningsdata

Möjliga konsekvenser av brister

Klass 0	Inga konsekvenser
Klass 1	kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part
Klass 2	kan orsaka omfattande obehag eller ekonomisk förl
Klass 3	kan medföra skada på liv eller hälsa för enskilda per skada för universitetet eller tredje part



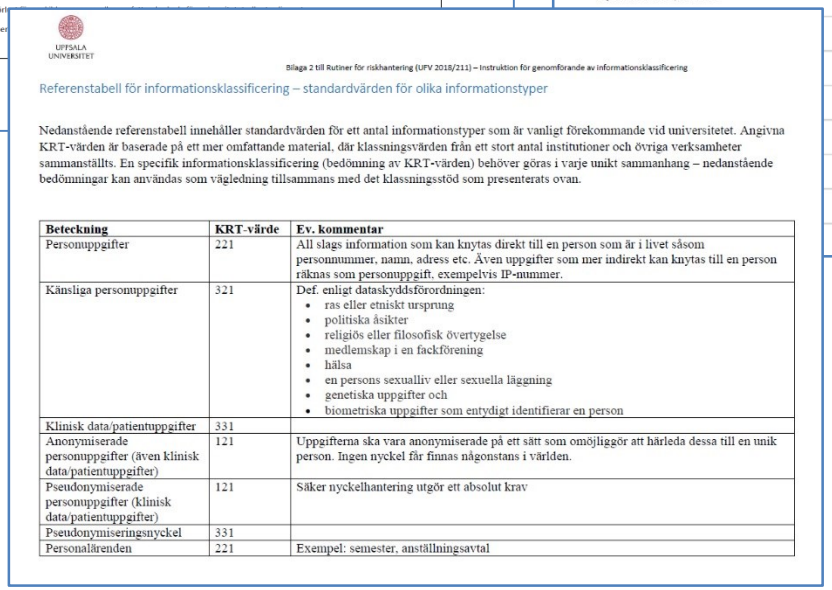
UPPSALA UNIVERSITET

Bilaga 2 till Rutiner för riskhantering (UFV 2018/211) – Instruktion för genomförande av informationsklassificering

Klassningsvärden för centrala system

Ett systems klassningsvärde (KRT-värde) bygger på det högsta klassningsvärdet för respektive aspekt (konfidentialitet, riktighet och tillgänglighet) som påträffas bland de informationsmängder som systemet hanterar. I momentet kravanalys säkerställs att systemet lever upp till en säkerhetsnivå som motsvarar systemets klassningsvärde. Efter dialoger med olika delar av verksamheten har informationsklassificeringar och kravanalyser för centrala system genomförts, detta inom ramen för universitetets centrala förvaltningsorganisation – se https://mp.uu.se/web/info/vart-uu/e-forvaltning. Nedan listas klassningsvärden för ett antal centrala system som har en tydlig koppling även till institutioners verksamhet.

System	Informationsklassning (KRT)	e-område
AKKA	332	Katalog och integration
Nya Raindance, RD2018	321	Ekonomi och inköp
	221	Forskningsadministration
	221	Forskningsadministration
	321	HR
	221	LOSAK
	322	Lärande och utbildning
	322	Lärande och utbildning



UPPSALA UNIVERSITET

Bilaga 2 till Rutiner för riskhantering (UFV 2018/211) – Instruktion för genomförande av informationsklassificering

Referenstabell för informationsklassificering – standardvärden för olika informationstyper

Nedanstående referenstabell innehåller standardvärden för ett antal informationstyper som är vanligt förekommande vid universitetet. Angivna KRT-värden är baserade på ett mer omfattande material, där klassningsvärden från ett stort antal institutioner och övriga verksamheter sammanställts. En specifik informationsklassificering (bedömning av KRT-värden) behöver göras i varje unikt sammanhang – nedanstående bedömningar kan användas som vägledning tillsammans med det klassningsstöd som presenterats ovan.

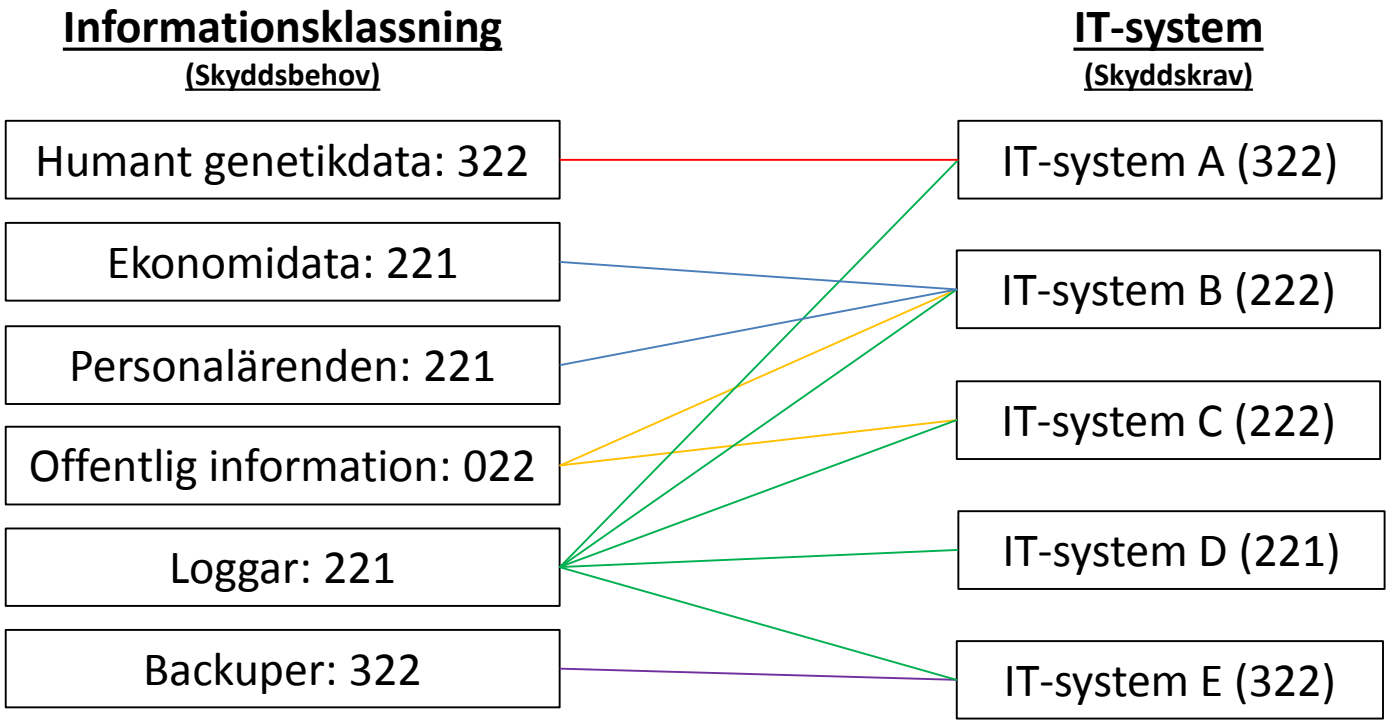
Beteckning	KRT-värde	Ev. kommentar
Personuppgifter	221	All slags information som kan knytas direkt till en person som är i livet såsom personnummer, namn, adress etc. Även uppgifter som mer indirekt kan knytas till en person räknas som personuppgift, exempelvis IP-nummer.
Känsliga personuppgifter	321	Def. enligt dataskyddsförordningen: • ras eller etniskt ursprung • politiska åsikter • religiös eller filosofisk övertygelse • medlemskap i en fackförening • hälsa • en persons sexualliv eller sexuella läggning • genetiska uppgifter och • biometriska uppgifter som entydigt identifierar en person
Klinisk data/patientuppgifter	331	
Anonymiserade personuppgifter (även klinisk data/patientuppgifter)	121	Uppgifterna ska vara anonymiserade på ett sätt som omöjliggör att härleda dessa till en unik person. Ingen nyckel får finnas någonstans i världen.
Pseudonymiserade personuppgifter (klinisk data/patientuppgifter)	121	Säker nyckelhantering utgör ett absolut krav
Pseudonymiseringsnyckel	331	
Personalärenden	221	Exempel: semester, anställningsavtal

UPPSALA UNIVERSITET

Klassningsprocessen

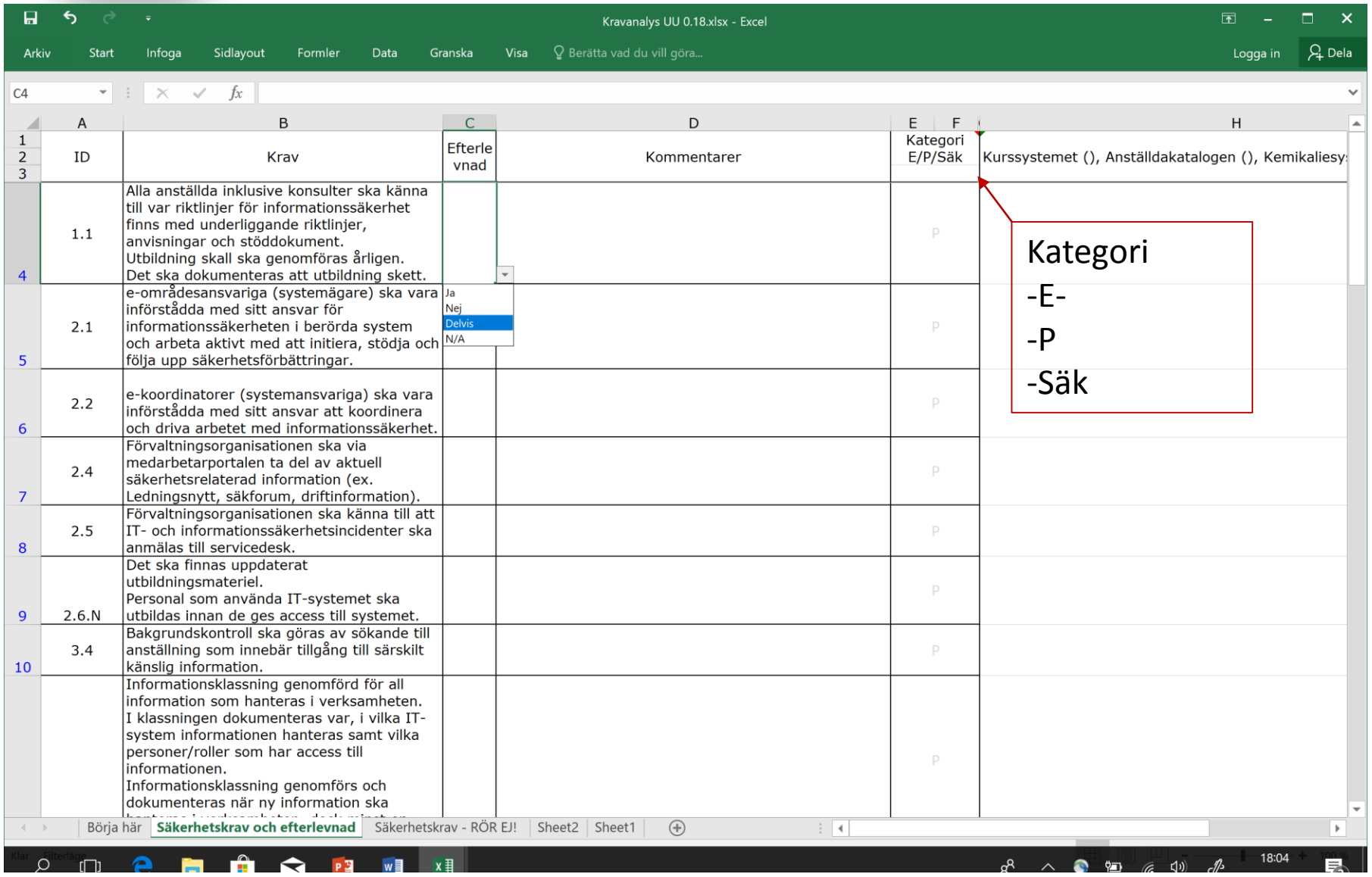
”Är systemet tillräckligt säkert för min information?”

Ger stöd i mappningen mellan informationens behov och vad IT-systemet uppfyller.



UPPSALA UNIVERSITET

Kravanalys (nästa steg) – att inventera och åtgärda brister i säkerhetsskyddet i de system som behandlar personuppgifter.



ID	Krav	Efterlevnad	Kommentarer	Kategori E/P/Säk	Kurssystemet (), Anställdakatalogen (), Kemikaliesy
1.1	Alla anställda inklusive konsulter ska känna till var riktlinjer för informationssäkerhet finns med underliggande riktlinjer, anvisningar och stöddokument. Utbildning skall ska genomföras årligen. Det ska dokumenteras att utbildning skett.			P	
2.1	e-områdesansvariga (systemägare) ska vara införstådda med sitt ansvar för informationssäkerheten i berörda system och arbeta aktivt med att initiera, stödja och följa upp säkerhetsförbättringar.			P	
2.2	e-koordinatorer (systemansvariga) ska vara införstådda med sitt ansvar att koordinera och driva arbetet med informationssäkerhet.			P	
2.4	Förvaltningsorganisationen ska via medarbetarportalen ta del av aktuell säkerhetsrelaterad information (ex. Ledningsnytt, säkforum, driftinformation).			P	
2.5	Förvaltningsorganisationen ska känna till att IT- och informationssäkerhetsincidenter ska anmälas till servicedesk.			P	
2.6.N	Det ska finnas uppdaterat utbildningsmateriel. Personal som använda IT-systemet ska utbildas innan de ges access till systemet.			P	
3.4	Bakgrundskontroll ska göras av sökande till anställning som innebär tillgång till särskilt känslig information.			P	
	Informationsklassning genomförd för all information som hanteras i verksamheten. I klassningen dokumenteras var, i vilka IT-system informationen hanteras samt vilka personer/roller som har access till informationen. Informationsklassning genomförs och dokumenteras när ny information ska			P	

UPPSALA UNIVERSITET

Inte bara system

Klassningen behöver ligga till grund för all informationshantering

- säkerställa att personuppgifter i system och tjänster och i all övrig hantering behandlas i enlighet med EU:s dataskyddsförordning vad avser säkerhetsmässiga aspekter

  säkerställa att all hantering av personuppgifter svarar mot universitetets krav på god informationssäkerhet

Behöver jag den här informationen?

Kan jag lägga den här informationen i Dropbox?

Måste jag lagra/kommunicera informationen krypterat?

Kan jag skicka denna information via e-post?

Rutiner för säker informationshantering

”… Informationshantering kan i många fall påverkas även av juridiska aspekter. Detta dokument avser att avgränsat hantera **informationssäkerhetsmässiga aspekter** …”

Omfattning:

4.1	Information i IT-system och lagringslösningar
4.2	Användning av molntjänster
4.3	Övrig informationshantering
4.4	Regler för säker informationshantering

Vad får jag göra med min information?
De regler som presenteras under 4.4 tar sin utgångspunkt i resultatet från genomförd informationsklassificering:

UPPSALA UNIVERSITET

4.4 Regler för säker informationshantering

4.4.1 Konfidentialitet

Regler klass 2

Informationen får lagras på arbetsstationens lokala hårddisk eller flyttbart medium under förutsättning att enheten hanteras i enlighet med anvisningar i avsnittet 4.2.3, *Eget ansvar/personligt förhållningssätt.* Därtill får informationen, under vissa förutsättningar, lagras i molntjänst. För bedömning om det är lämpligt att lagra informationen i en molntjänst - se punkten 4.2, Användning av molntjänster, eller kontakta universitetets informationssäkerhetssamordnare för vägledning.

Informationen får lagras på en filserver placerad i ett serverrum med accesskontroll.

Informationen skall vid elektronisk överföring, exempelvis via e-post eller webb, krypteras innan den överförs externt (utanför universitetet).

Informationen får göras tillgänglig för extern åtkomst endast via VPN-lösning eller motsvarande.

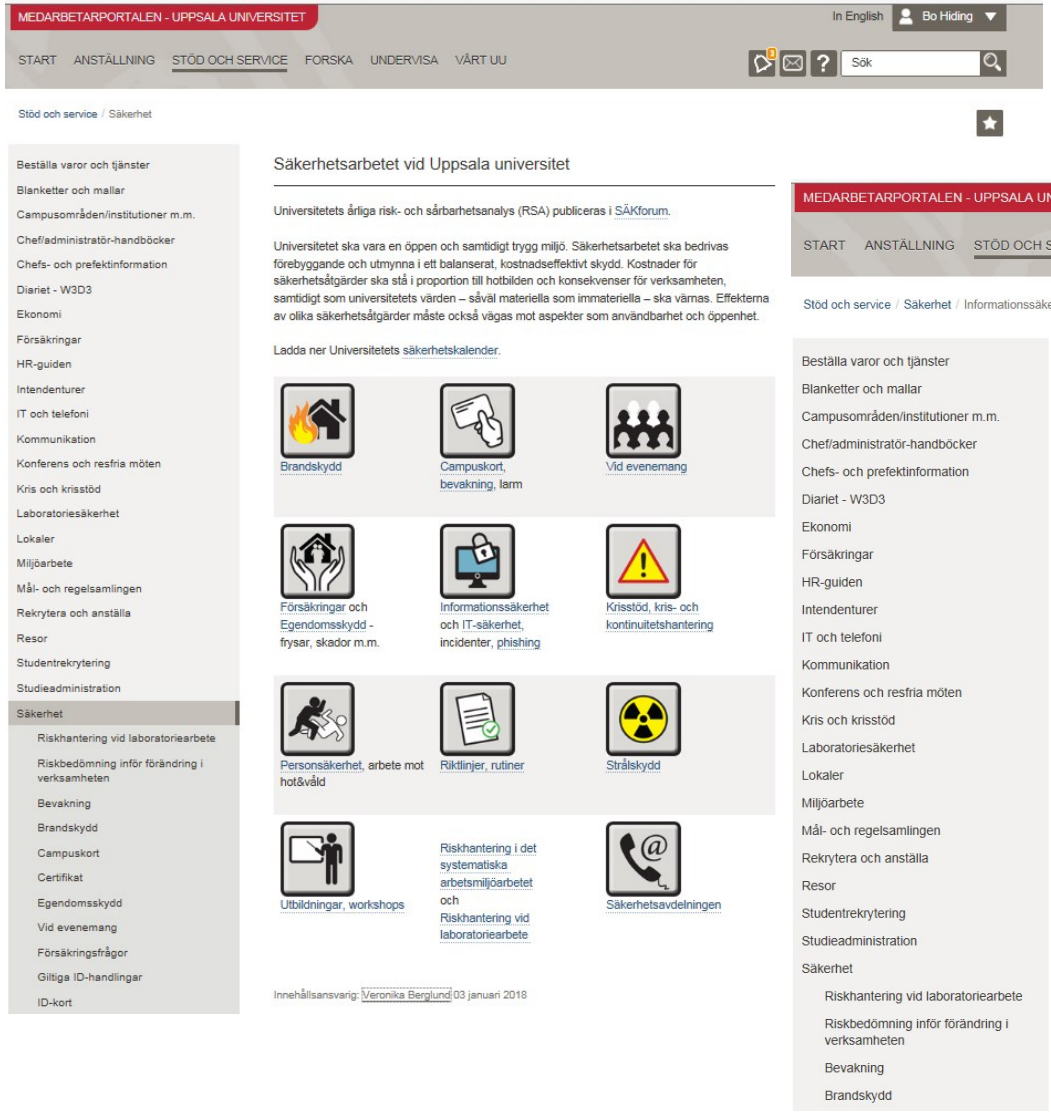
Informationen får sändas via fax och med post, såväl internt som externt.

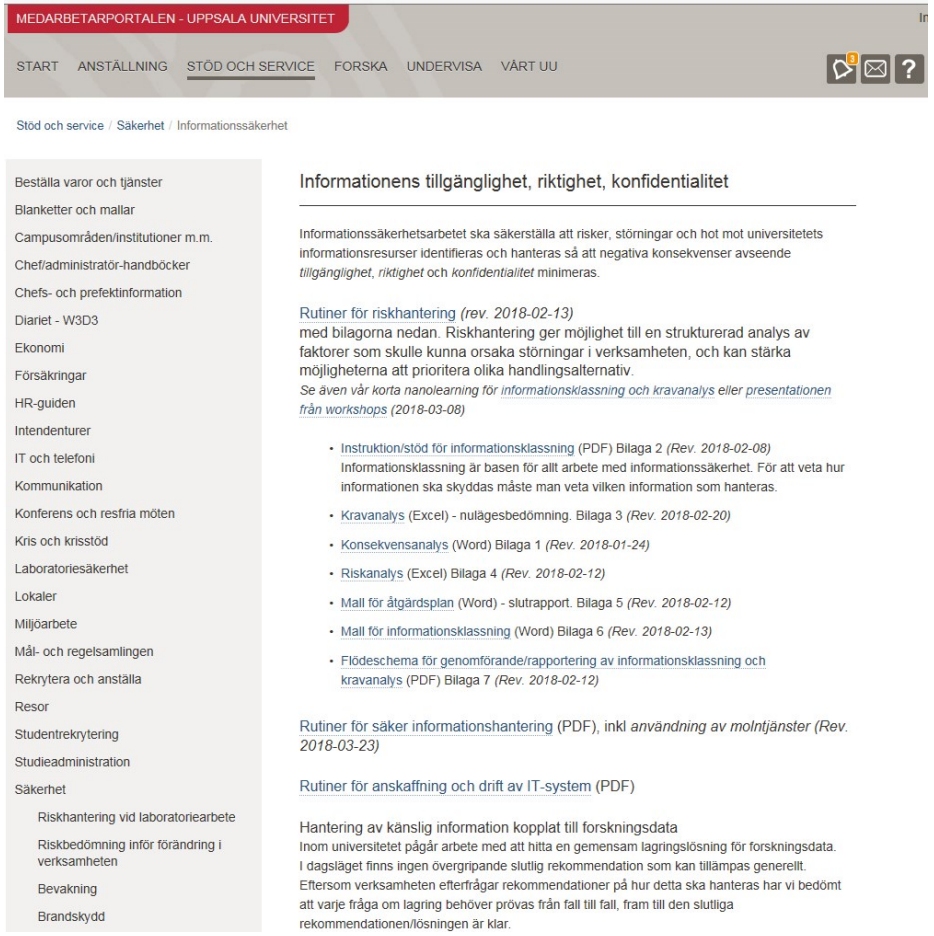
Vid byte av hårddisk skall all information på den utrangerade skrivas över på sådant sätt att den inte kan återskapas.

UPPSALA UNIVERSITET

Kolla in våra sidor i Medarbetarportalen

https://mp.uu.se/web/info/stod/sakerhet

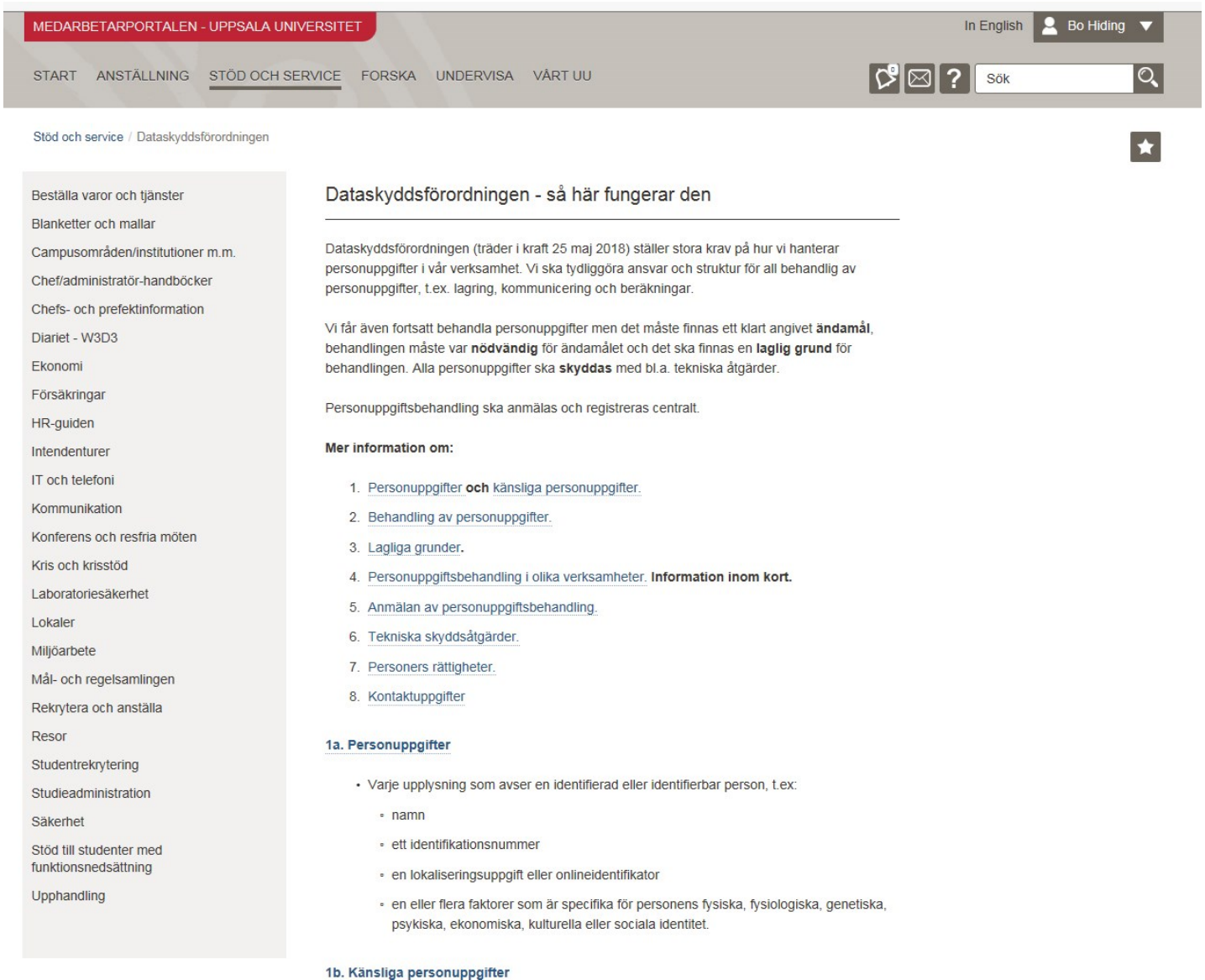




UPPSALA UNIVERSITET

Kolla in våra sidor i Medarbetarportalen

https://mp.uu.se/web/info/stod/dataskyddsforordningen



Workshop – vad ska vi göra?

1.2 Klassificeringstabell

ID	Beteckning	Förklaring	IT-system (ägare)	Roller	KRT värde	Motivering

- Använd blankett enligt ovan som underlag för arbetet (Rutiner för riskhantering – bilaga 6)
- Inventera vilka informationsmängder som ni hanterar i er verksamhet – ange en informationsmängd per rad i kolumnen Beteckning. Använd gärna kolumnen Förklaring för tydliggöranden gällande den aktuella informationsmängden. Ange vilka roller som hanterar informationen i särskild kolumn.
- I kolumnen IT-system (ägare) – ange vilka system som hanterar den aktuella informationsmängden. Ange även hur informationen lagras/hanteras i övrigt (ex: lagras på USB-disk, skickas via e-post etc.)
- Klassificera varje identifierad informationsmängd enligt instruktion

Not. Utdelat stöddokument (Rutiner för riskhantering – bilaga 2) samt utdelat exempel ger vägledning i arbetet.

UPPSALA UNIVERSITET

Information som återkommer

Vi testar en idé som utgår från en standardklassificering

1.2 Klassificeringstabell

Nedan finns en version av klassificeringstabellen där de informationstyper som vanligtvis hanteras vid varje institution är förifylld med en standardklassificering. Fyll i uppgift om lokal informationsanvändning vid institutionen i kolumnen *IT-system (ägare)* samt ange vilka roller som hanterar informationen i särskild kolumn avsedd för denna uppgift. Gör detta för varje informationstyp som förekommer vid er institution och bedöm huruvida standardklassificeringen (*KRT-värdet)* stämmer med er egen klassificering. Vid ändring av KRT-värde – ange motivering till ändringen i särskild kolumn. För vägledning och information angående övrig standardklassificering - se Bilaga 2 till Rutiner för riskhantering (UFV 2018/211).

Efter bedömning av förifyllda informationstyper – komplettera med övrigt som hanteras vid institutionen.

ID	Beteckning	Förklaring	IT-system (ägare)	Roller	KRT värde	Motivering
	Personuppgifter	All slags information som kan knytas direkt till en person som är i livet såsom personnummer, namn, adress etc. Även uppgifter som mer indirekt kan knytas till en person räknas som personuppgift, exempelvis IP-nummer.	Finns i centrala system som exempelvis Akka, Uppdok, Primula m.fl: Övrig lokal anv		221	
	Känsliga personuppgifter	Def. enligt dataskyddsförordningen: • Ras eller etniskt ursprung • Politiska åsikter • Religiös eller filosofisk övertygelse • Medlemskap i en fackförening • Hälsa	Finns i centrala s exempelvis Akk Primula p Övrig lokal anv			

För varje informationstyp som används:

- Ange var/hur informationen används lokalt vid institutionen
- Ange vilka roller som hanterar informationen lokalt
- Bedöm huruvida standardklassificeringen stämmer och motivera ev. avvikelser från standardvärden

Efter bedömning av förifyllda informationstyper – komplettera med övrigt som hanteras vid institutionen.

UPPSALA UNIVERSITET

… och sen då

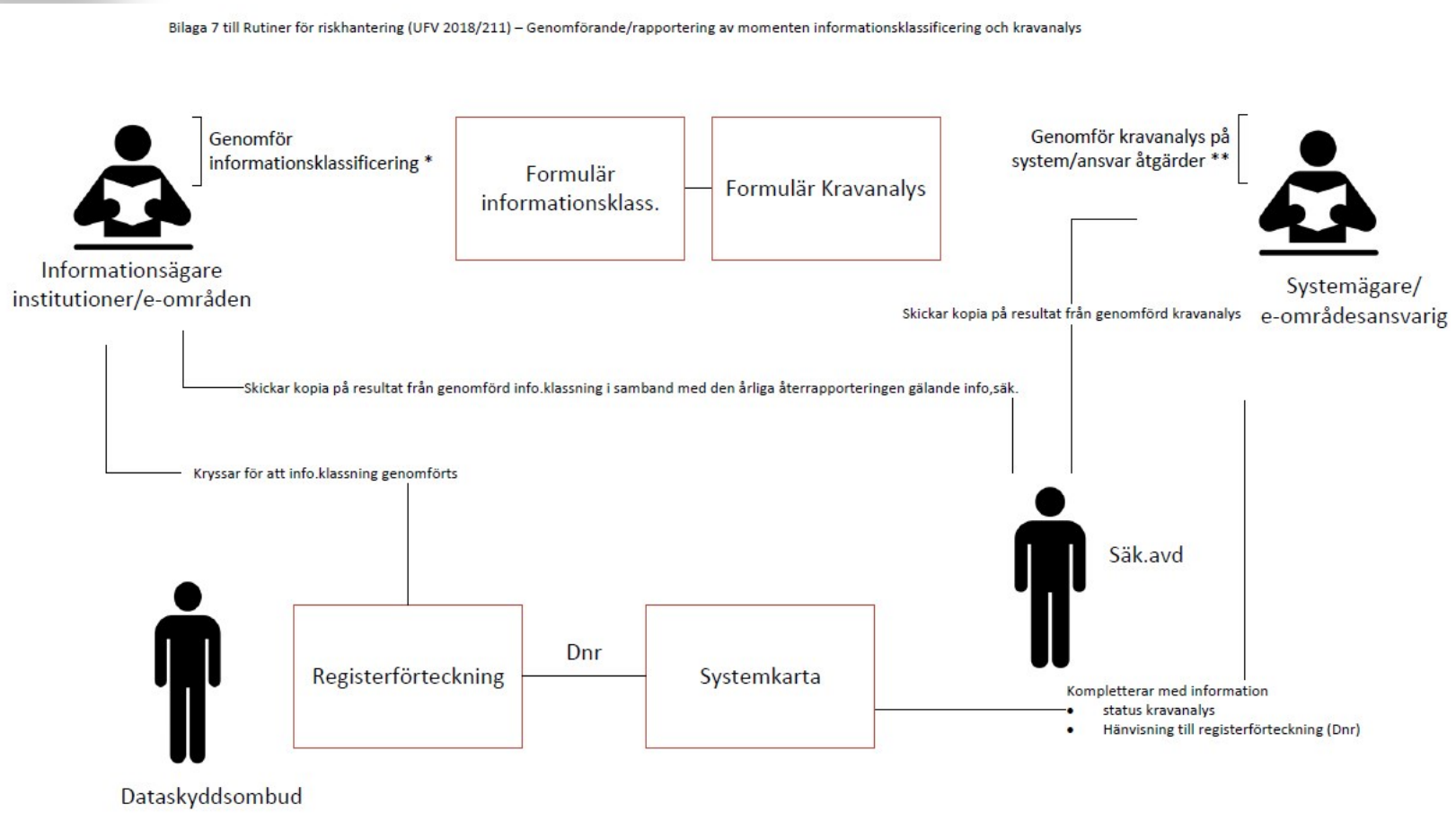
- Har vi lokala system ska en kravanalys genomföras för att tillse att informationen i systemet omgärdas med tillräcklig säkerhet. Rutiner för riskhantering – bilaga 3 utgör verktyg i sammanhanget. Universitetets informationssäkerhetssamordnare hjälper gärna till.

- Resultatet från informationsklassificering och ev. kravanalyser ägs av institutionen och hanteras som ett levande dokument (utgör grund för lokal kommunikation angående säker informationshantering, utgör underlag vid förnyade bedömningar årligen, används i det kontinuerliga arbetet med förbättringsåtgärder.

- Kopior av resultatet sänds till säkerhetsavdelningen för samordning av åtgärder gällande återkommande brister.

UPPSALA UNIVERSITET

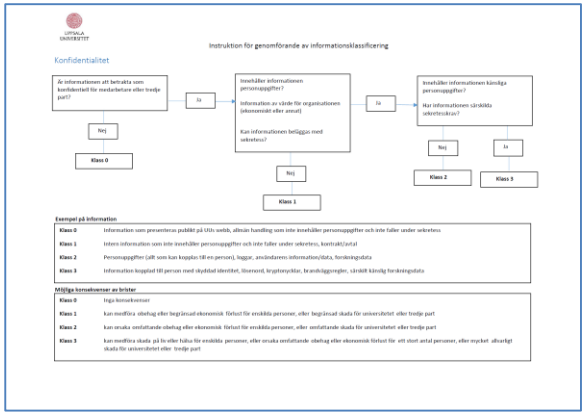
Genomförande och rapportering



** Genomförs med bilaga 6 som underlag enligt instruktioner i bilaga 2*
*** Genomförs med stöd av bilaga 3*

Vid en institution kan rapporteringsmomenten lämpligen samordnas via prefekten.

Att ta med sig till det fortsatta arbetet vid institutionen


Instruktion för genomförande av informationsklassificering

Konfidentialitet

Är informationen att betrakta som konfidentiell för medarbetare eller tredje part?

Ja

Innehåller informationen personuppgifter?

Information av värde för organisationen (ekonomiskt eller annat)

Kan informationen beläggas med sekretess?

Ja

Innehåller informationen känsliga personuppgifter?

Har informationen särskilda sekretesskrav?

Nej

Klass 0

Nej

Klass 1

Nej

Klass 2

Ja

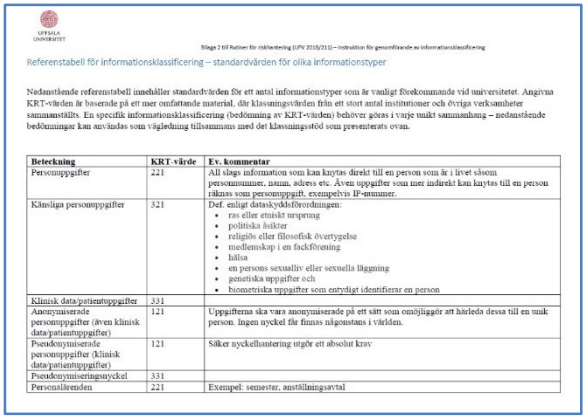
Klass 3

Exempel på information

Klass 0	Information som presenteras publikt på UUs webb, allmän handling som inte innehåller personuppgifter och inte faller under sekretess
Klass 1	Intern information som inte innehåller personuppgifter och inte faller under sekretess, kontrakt/avtal
Klass 2	Personuppgifter (allt som kan kopplas till en person), loggar, användarens information/data, forskningsdata
Klass 3	Information kopplad till person med skyddad identitet, lösenord, krypteringsnycklar, brandväggsregler, särskilt känslig forskningsdata

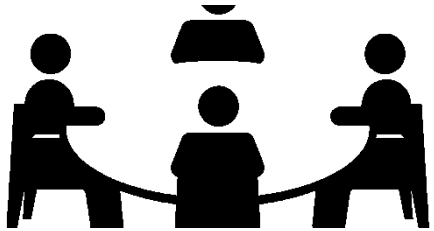
Möjliga konsekvenser av brister

Klass 0	Inga konsekvenser
Klass 1	kan medföra obehag eller begränsad ekonomisk förlust för enskilda personer, eller begränsad skada för universitetet eller tredje part
Klass 2	kan orsaka omfattande obehag eller ekonomisk förlust för enskilda personer, eller omfattande skada för universitetet eller tredje part
Klass 3	kan medföra skada på liv eller hälsa för enskilda personer, eller orsaka omfattande obehag eller ekonomisk förlust för ett stort antal personer, eller mycket allvarligt skada för universitetet eller tredje part


Bilaga 2 till Rutiner för riskhantering (UFV 2018/211) – Instruktion för genomförande av informationsklassificering

Referenstabell för informationsklassificering – standardvärden för olika informationstyper

Nedanstående referenstabell innehåller standardvärden för ett antal informationstyper som är vanligt förekommande vid universitetet. Angivna KRT-värden är baserade på ett mer omfattande material, där klassningsvärden från ett stort antal institutioner och övriga verksamheter sammanställts. En specifik informationsklassificering (bedömning av KRT-värden) behöver göras i varje unikt sammanhang – nedanstående bedömningar kan användas som vägledning tillsammans med det klassningsstöd som presenterats ovan.

Beteckning	KRT-värde	Ev. kommentar
Personuppgifter	221	All slags information som kan kopplas direkt till en person som är i livet såsom personnummer, namn, adress etc. Även uppgifter som mer indirekt kan kopplas till en person räknas som personuppgift, exempelvis IP-nummer.
Känsliga personuppgifter	321	Def. enligt dataskyddsförordningen: • ras eller etniskt ursprung • politiska åsikter • religiös eller filosofisk övertygelse • medlemskap i en fackförening • hälsa • en persons sexualliv eller sexuella läggning • genetiska uppgifter och • biometriska uppgifter som entydigt identifierar en person
Klinisk data/patientuppgifter	331	
Anonymiserade personuppgifter (även klinisk data/patientuppgifter)	121	Uppgifterna ska vara anonymiserade på ett sätt som omöjliggör att härleda dessa till en unik person. Ingen nyckel får finnas någonstans i världen.
Pseudonymiserade personuppgifter (klinisk data/patientuppgifter)	121	Säker nyckelhantering utgör ett absolut krav
Pseudonymiseringsnyckel	331	
Personalärenden	221	Exempel: semester, anställningsavtal

- Hitta rätt nivå på klassningen. Vi behöver inte klassa informationen på termnivå. Utdelade stöddokument ger vägledning att hitta rätt nivå
- Använd gärna workshopformen - samla grupperingar som representerar olika områden
- Sammanställ resultatet (inte en blankett till varje forskare)
- Vi erbjuder hjälp i det lokala arbetet