UMEÅ UNIVERSITET

VÄGLEDNING

INFORMATIONSKLASSNING OCH RISK- OCH SÅRBARHETSANALYS

Revidering 20220601	Harmonisering av antal nivåer (1-4) i KRT-modeller med motsvarande nivåer i risk och sårbarhetsanalys.	D.Harnesk
20220607	Kompletterat med exempel på säkerhetsåtgärder för Konfidentialiet och Riktighet, nivå 2-4	D.Harnesk

UMEÅ UNIVERSITET

Innehåll

1. Beskrivning

Dokumentet beskriver tillvägagångssätt för informationsklassning samt risk- och sårbarhetsanalys som gäller vid Umeå universitet. Dokumentet består av två delar: del 1 Informationsklassning och del 2 Risk- och sårbarhetsanalys.

Mallar för dokumentation återfinns i Aurora under Informationssäkerhet och rubriken vägledande dokument.

2. Del 1 – Informationsklassning bakgrund

Syftet med att klassificera information med avseende på säkerhetsaspekterna Konfidentialitet, Riktighet, Tillgänglighet, som kompletteras med risk-och sårbarhetsanalys för att bedöma och fastställa kraven på hur universitets information och berörda informationssystem ska hanteras med avseende på säkerhetsåtgärder. Ansvar och roller kopplade till informationssäkerhet och informationsklassning beskrivs i *Regel- informationssäkerhet*.

Resurser som används för att hantera informationen, till exempel it-system, it-infrastruktur och fysiska tillgångar ska möta kraven som klassningen medför. De resurser som hanterar informationen behöver därför skyddas på lägst den nivå som högst klassad information har.

Särskilt om klassning och säkerhetsskyddslagen

Säkerhetsskyddsklassificerade uppgifter rör säkerhetskänslig verksamhet i enlighet med säkerhetsskyddslagstiftningen. Om säkerhetsskyddsklassificerade uppgifter förekommer universitetets säkerhetschef kontaktas.

3. Definitioner

Det som klassas vid ett specifikt tillfälle kallas *informationsbehandling* eller informationstillgång. Dessa genomförs/används av en meningsfull aktivitet i organisationen exempelvis på en enhet eller avdelning, en process, en tjänst, it-system, eller ett forskningsprojekt.

I en *informationsbehandling* ingår ofta en grupp av uppgifter som kan finnas lokalt i en verksamhet/forskningsprojekt eller vara spridd över hela organisationen, som exempelvis personuppgifter. Flera forskningsprojekt inom en fakultet eller institution kan också hantera samma typ av informationsbehandling, som exempelvis *datainsamling*. Uppgifter som ingår i datainsamling är till exempel: *enkät, intervju, olika mätvärden, kvalitetsregister*.

4. Användningsområden

Tillfällen när informationsklassning bör ligga till grund för val av lämpliga skyddsåtgärder är:

- Inför personuppgiftsbehandlingar
- Bedömning hur forskningsmaterial/data ska hanteras och därmed skyddas
- Nulägesbedömning och/eller riskanalys genomförs av ett informationssystem
- Anskaffning, nyutveckling eller förändring av it-system eller infrastruktur, t.ex. datalagrings-tjänster
- Fastställande av säkerhetsdesign av ett informationssystem
- Förändringar av rättsliga krav
- Nytillkommen information i verksamheten
- Fastställande av hanteringsregler av information, t.ex. med avseende på krav på kryptering av e-post, regler för kommunikation via mobiltelefon, etc.

Nedanstående klassningsmodeller (tabell 1-3) är baserade på Umeå universitets informationssäkerhetspolicy, it-säkerhetsplan, Dataskyddsförordningen, MSB:s föreskrifter och allmänna råd om statliga myndigheters informationssäkerhet samt det metodstöd för informationssäkerhet som tillhandahålls av MSB.

Konfidentialitet (K) tabell 1

Konfidentialitet (K)	**Skyddsnivå**	**Konsekvens av bristande skydd**
Vad kan konsekvenserna bli ifall obehöriga får åtkomst till uppgifterna	**Nivå 1**: Informationen är publik och kräver inget skydd	**Inga** konsekvenser
	Nivå 2: Informationen kräver grundläggande skydd	**Måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Enstaka missnöjda samarbetspartners, uttryck i sociala medier. Lindrig förtroendeskada
	Nivå 3: Informationen kräver högt skydd –	**Betydande** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Begränsat missnöje, uttryckt i riks- och lokalmedia. Betydande förtroendeskada hos samarbetspartners eller hos allmänheten.
	Nivå 4: Informationen kräver mycket högt skydd	**Allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Flertalet missnöjda samarbetspartners, drev i riksmedier el sociala grupper. Allvarlig förtroendeskada
Hanteras information som faller under säkerhetsskyddslagen (2018:585), eller produkter med dubbla användningsområden så ska säkerhetssamordnare vid lokalförsörjningsenheten kontaktas.		

Tabell 1.

Riktighet (R) tabell 2

Riktighet (R)	Skyddsnivå	Konsekvenser av brister i riktighet
Vad kan konsekvenserna bli ifall uppgifterna är felaktiga eller inaktuella	**Nivå 1**: Informationen kräver inget skydd	**Inga** konsekvenser
	Nivå 2: Riktighetskravet på informationen är måttligt	**Måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Enstaka missnöjda samarbetspartners, uttryck i sociala medier. Lindrig förtroendeskada
	Nivå 3: Riktighetskravet på informationen är högt	**Betydande** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Begränsat missnöje, uttryckt i riks- och lokalmedia. Betydande förtroendeskada hos samarbetspartners eller hos allmänheten.
	Nivå 4: Riktighetskravet på informationen är mycket högt	**Allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Flertalet missnöjda samarbetspartners, drev i riksmedier el sociala grupper. Allvarlig förtroendeskada

Tabell 2

Tillgänglighet (T) tabell 3

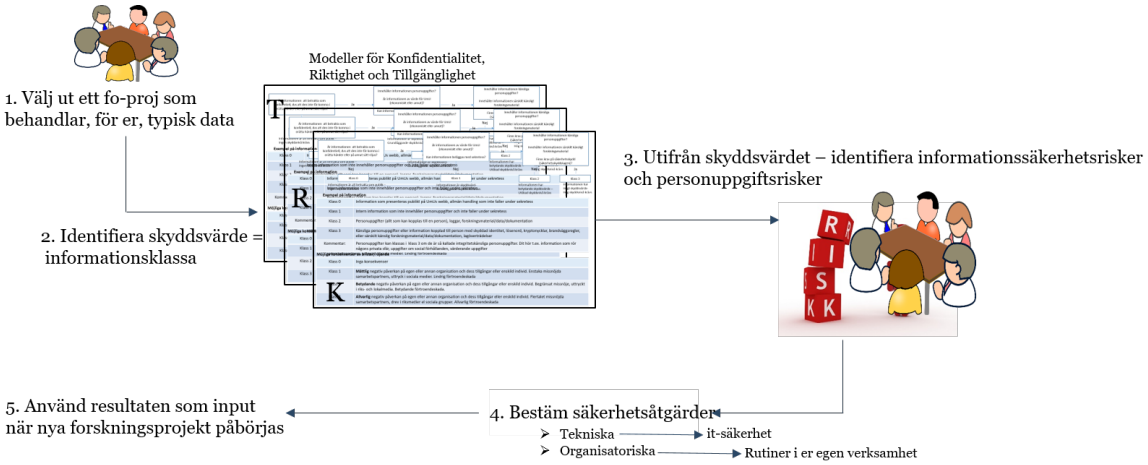
Tillgänglighet (T)	Skyddsnivå	Konsekvens av bristande tillgänglighet
Vad kan konsekvenserna bli ifall någon (som är behörig) inte får tillgång till uppgifterna?	**Nivå 1**	Inga konsekvenser
	Nivå 2: Tillgång till informationen kräver grundläggande skydd	Avbrott i system medför lindrig påverkan på verksamheten
	Nivå 3: Tillgång till informationen kräver högt skydd	Avbrott i system kräver stora omprioriteringar i verksamheten
	Nivå 4: Tillgång till informationen kräver mycket högt skydd	Förlust av data ger mycket höga återställningskostnader i tid och pengar

Tabell 3

5. Genomför klassning

Deltagare från verksamheten bör tillsammans ha kunskap om vilken information som finns i klassningsobjektet (forskningsstudier, it-system, verksamhetsprocesser, externa datalagringstjänster, etc.). Finns tidigare genomförda klassningar kan man med fördel ta stöd från dessa inför en ny situation. Observera att detta avsnitt exemplifieras med forskningsverksamhet men gäller även för all annan informationshantering.

Figur 4 innehåller steg som är nödvändiga för att hantera information på ett säkert sätt vid Umeå universitet. Inom en institutions forskningsverksamhet kan det vara så att forskningsstudierna nästan alltid samlar in, analyserar och publicerar en och samma övergripande typ av data. Det kan till exempel vara Hälsodata som utgörs av olika variabler, mätvärden, etc. Hälsodata handlar alltid om data med högsta skyddsvärde, enligt Integritetsmyndighetens definition vad känsliga personuppgifter är.



Figur 4. Angreppssätt informationsklassning och riskbedömning

För att komma igång med informationsklassning är det lämpligt att välja ett, för institutionen, typiskt forskningsprojekt. Låt det projektet vara exempel på vanligast förekommande forskningsdata (1). Gör en informationsklassning genom att använda er av mallarna för konfidentialitet, riktighet och tillgänglighet och bestäm skyddsvärde (2). Att klassa informationstillgångar innebär att man gör en konsekvensbedömning för vad som kan hända om informationens konfidentialitet, riktighet och tillgänglighet inte upprätthålls i den utsträckning verksamheten behöver. Se bilaga för exempel på informationstillgångar d.v.s. information som hanteras i den fortlöpande verksamheten.

Exempel på frågor man kan ställa sig:

- *Konfidentialitet*: Vad kan konsekvenserna bli ifall informationen läcker ut till obehöriga?
- *Riktighet*: Vad kan konsekvenserna bli ifall informationen är felaktig eller inaktuell?
- *Tillgänglighet*: Vad kan konsekvenserna bli ifall någon (som är behörig) inte får tillgång till informationen?

Dokumentera klassningen. Använd excelmall för forskningsprojekt eller för it-system om informationsbehandlingen avser verksamhetssystem.

När klassning är dokumenterad med identifierat skyddsvärde och konsekvenser är det dags att identifiera informationssäkerhetsrisker och personuppgiftsrisker (3). Exempel när risker kan uppstå:

- Genom att använda publika molntjänster
- Genom att dela känsligt forskningsdata/material via okrypterade kanaler.
- Genom att inte följa universitetets tips och råd för resesäkerhet

I dessa exempel är informationssäkerhetsrisker i form av röjande och förvanskning av forskningsdata stora. Likaledes om data innehåller känsligt hälsodata är personuppgiftsrisker överhängande och enskilda individers integritetsskydd försvagas. För att dokumentera informations- och personuppgiftsrisker genomför risk och sårbarhetsanalys enligt del 2 i denna vägledning.

Umeå universitets krav är att använda interna verifierade lagringsytor och samarbetsytor för delning av information för säker informationshantering. Se vidare i Lathund digitala arbets- och lagringsytor för personal vid Umeå universitet. (4) Vidare innehåller lathunden tips på grundläggande tekniska och organisatoriska säkerhetsåtgärder för respektive klassningsnivå.

Här finns ytterligare information om dataskyddsförordningen och olika personuppgifter.

6. Exempel säkerhetsåtgärder

Säkerhetsåtgärder kopplade till samarbete och lagringsytor			
Hanteringsregler	**Exempel på data och konsekvens vid förlust/röjande/obehörig åtkomst samt av data, samt inkorrekt data**	**Allmänt för alla klassningsnivåer: Grundläggande säkerhetsåtgärder är att begränsa åtkomst till it-resurser och minimera risk för röjande och förvanskning av information.**	
		it-säkerhetsåtgärd	**Organisatorisk säkerhetsåtgärd**
Klass 2 – Information kräver grundläggande skydd Informationen får lagras och överföras på och med alla grönmarkerade tjänster som gäller för klassningsvärde 2. .	Information för UmU:s fortlöpande verksamhet som innehåller vanliga personuppgifter, och information som inte faller under sekretess, eller andra förekomster av konfidentialitetsavtal **Måttlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Enstaka missnöjda samarbetspartners, uttryck i sociala medier. Lindrig förtroendeskada	Grundläggande skydd säkerställs genom inloggning till it-resurser med UmU-ID eller motsvarande. Ytterligare grundläggande skydd erhålls genom tjänsten klienthantering av personaldatorer.	Användare ska endast ges tillgång till it-resurser och it-tjänster som de specifikt beviljats tillstånd för. Institutioner och enheter har rutin för att regelbundet identifiera, ta bort eller inaktivera överflödiga behörigheter. Mottagare av information ska alltid vara känd
Klass 3 – Information kräver högt skydd Informationen får lagras och överföras på och med alla grönmarkerade tjänster som gäller för klassningsvärde 3. Därtill får informationen, under vissa förutsättningar lagras i Microsofts molntjänst. För bedömning om det är lämpligt kontakta ITS/infosäk för vägledning.	Integritetskänsliga personuppgifter Information som är kritisk för t.ex. en enskild forskare, forskargrupp, forskningsprojekt **Betydande** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Begränsat missnöje, uttryckt i riks- och lokalmedia. Betydande förtroendeskada	Högt skydd säkerställs genom att använda tjänsten Skyddad bilaga vid överföring av information externt, samt tjänsten Skyddade dokument för dokumentlagring. Högt skydd säkerställs genom 2-faktorsautenticering. Högt skydd säkerställs med VPN för åtkomst utanför Umu till interna it-resurser.	*Användare ska endast ges tillgång till it-resurser och it-tjänster som de specifikt beviljats tillstånd för.* *Institutioner och enheter har rutin för att regelbundet identifiera, ta bort eller inaktivera överflödiga behörigheter.* *Mottagare av information ska alltid vara känd* Säkerställ att regler för användning av mobila enheter och vid distansarbete efterlevs.
Klass 4 – Information kräver mycket högt skydd Informationen får lagras och överföras på och med alla grönmarkerade tjänster som gäller för klassningsvärde 4. Information får sparas i tjänsten skyddade dokument och DIP. Informationen kan skickas externt med tjänsten skyddad bilaga. Vid samarbete och lagring av information som faller under säkerhetsskyddslagen ska säkerhetssamordnare vid lokalförsörjningsenheten kontaktas.	Känsliga personuppgifter Information kopplad till person med skyddad identitet, Särskilt skyddsvärd information i forskningsverksamhet **Allvarlig** negativ påverkan på egen eller annan organisation och dess tillgångar eller enskild individ. Flertalet missnöjda samarbetspartners, drev i riksmedier eller sociala grupper. Allvarlig förtroendeskada.	Mycket högt skydd säkerställs genom att använda tjänsten Skyddad bilaga vid överföring av information externt, samt tjänsten Skyddade dokument för dokumentlagring. Mycket högt skydd säkerställs med VPN för åtkomst utanför Umu till interna it-resurser. Mycket högt skydd genom klienthantering med aktiverad lokal kryptering (Bitlocker, FileVault Vid behov av säkerhetsåtgärder som ger mycket högt skydd kontaktas ITS för vägledning.	*Användare ska endast ges tillgång till it-resurser och it-tjänster som de specifikt beviljats tillstånd för.* *Institutioner och enheter har rutin för att regelbundet identifiera, ta bort eller inaktivera överflödiga behörigheter* *Säkerställ att regler för användning av mobila enheter och vid distansarbete efterlevs.* *Mottagare av information ska alltid vara känd* KODNYCKEL till pseudonymiserade känsliga personuppgifter måste förvaras separat från källdata. Kodnyckel ska skyddas med multifaktorsautentisering och kontroll av behörighet. Dokumenterade rutiner för skydd av information vid användning av mobil it-utrustning.

7. Del 2 - Risk- och sårbarhetsanalys bakgrund

Del 2 beskriver hur en riskanalys går till.

Metoden går att använda vid en organisationsövergripande riskanalys eller vid en riskanalys av ett enskilt analysobjekt, till exempel en process eller ett it-system.

Innan riskanalysen påbörjas bör analysobjekt ha identifierats och den informationstillgång som ingår bör ha värderats genom informationsklassificering.

I riskanalysen identifieras de hot och oönskade händelser som kan påverka informationssäkerheten i organisationen. En riskanalys går ut på att besvara de tre frågorna; *Vad kan hända? Hur sannolikt är det? och Vad blir konsekvenserna?*

Syftet är att ge ett underlag för beslut om vilka säkerhetsåtgärder som ska införas men också att höja medvetenheten om hot, sårbarheter och risker hos de som deltar i analysen.

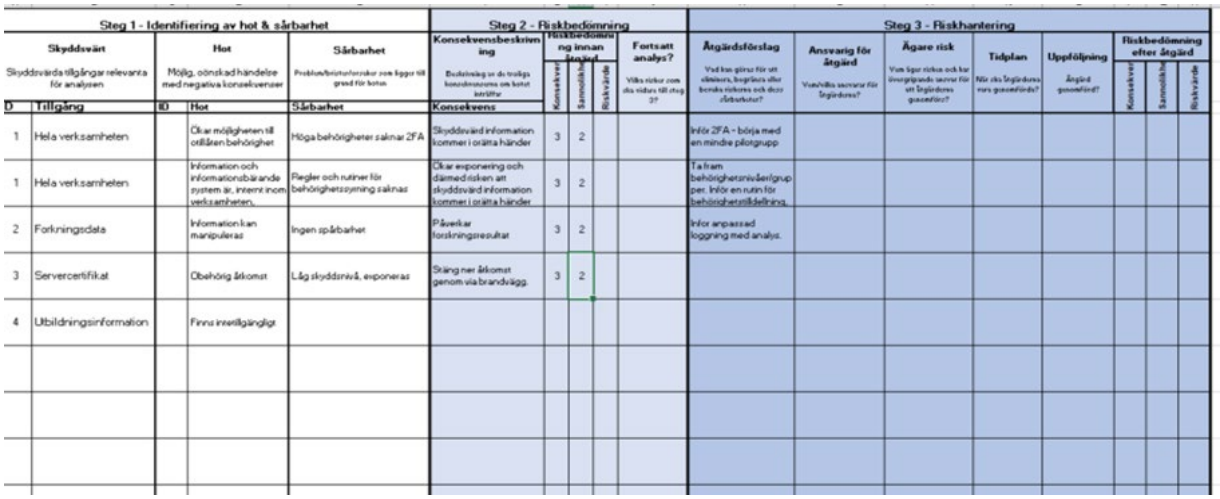
8. Användningsområden

Riskanalysens användningsområde är stort och kan genomföras på olika nivåer och situationer. Några exempel på analysobjekt:

- Verksamheten som helhet
- Vid nyanskaffning it-system/tjänst
- Ett forskningsprojekt
- En specifik informationsmängd
- En specifik applikation

- En serverhall
- En verksamhetsprocess
- En organisationsförändring

Nedanstående exempel på mall innefattar själva riskanalysen och ger även stöd för fortsatt arbete med hantering av de identifierade riskerna. Mallen finns tillgänglig på Aurora.



Steg 1 - Identifiering av hot & sårbarhet					Steg 2 - Riskbedömning					Steg 3 - Riskhantering							
Skyddsvärt		Hot		Sårbarhet	Konsekvensbeskrivning	Riskbedömning innan åtgärd			Fortsatt analys?	Åtgärdsförslag	Ansvarig för åtgärd	Ägare risk	Tidplan	Uppföljning	Riskbedömning efter åtgärd		
Skyddsvärda tillgångar relevanta för analysen		Möjlig, oönskad händelse med negativa konsekvenser		Problem/brister/svagheter som ligger till grund för hotet	Beskrivning av de troliga konsekvenserna om hotet inträffar	Konsekvens	Sannolikhet	Riskvärde	Vilka risker som ska vidare till steg 3?	Vad kan göras för att elimin., begränsa eller bemöta riskerna och deras sårbarheter?	Vem/vilka ansvarar för åtgärderna?	Vem ligger risken och har övergripande ansvar för att åtgärderna genomförs?	När ska åtgärderna vara genomförda?	Åtgärd genomförd?	Konsekvens	Sannolikhet	Riskvärde
ID	Tillgång	ID	Hot	Sårbarhet	Konsekvens												
1	Hela verksamheten		Ökar möjligheten till otillåten behörighet	Höga behörigheter saknar 2FA	Skyddsvärd information kommer i orätta händer	3	2			Inför 2FA - börja med en mindre pilotgrupp							
1	Hela verksamheten		Information och informationsbärande system är, internt inom verksamheten,	Regler och rutiner för behörighetstyrning saknas	Ökar exponering och därmed risken att skyddsvärd information kommer i orätta händer	3	2			Ta fram behörighetsnivåer/grupper. Inför en rutin för behörighetstilldelning.							
2	Forkningsdata		Information kan manipuleras	Ingen spårbarhet	Påverkar forskningsresultat	3	2			Inför anpassad loggning med analys.							
3	Servercertifikat		Obehörig åtkomst	Låg skyddsnivå, exponeras	Stäng ner åtkomst genom via brandvägg.	3	2										
4	Utbildningsinformation		Finns inetillgängligt														

9. Genomföra riskanalysen

1 Förbered så mycket som möjligt när det gäller beskrivning av analysobjektet. Resultat från informationsklassning nyttjas som en grund för den fortsatta riskanalysen.

2 Använd systembeskrivningar av den it-lösning som planeras att användas? Ta reda på vilka lagar och krav som kan påverka. Hur tas hänsyn till informationstillgångens livscykel?

3 **Steg 1 – Identifiering av hot och sårbarheter**. **Vad kan hända?**
Hotbild – använd generella och aktuella beskrivningar av hotbilder i exempelvis trend och årsrapporter (internationella, nationella och sektorsspecifika). Finns tidigare incidentsammanställningar inom organisationen att ta del av? Vilka hot och vilka sårbarheter har identifierats som kan medföra att en oönskad händelse kan inträffa och ge negativa konsekvenser?

Exempel hur hot, sårbarhet och risk hänger ihop:

Hot	**Sårbarhet**	**Risk**	**Informationstillgång**
Vem som helst kan gå in på mitt kontor.	Min kontorsdörr är olåst	Min arbetsdator stjäls	Min arbetsdator
Cyberattack	Känsliga person-uppgifter (t.ex. hälsodata) lagras i publik moln-tjänst	Känsliga person-uppgifter kommer i orätta händer	Forskningsdata

4 Steg 2 – Riskbedömning. Lista riskerna – numrera

Riskbedöm genom att titta på sannolikhet och konsekvens för varje risk.

Konsekvens		Sannolikhet	Intervall sannolikhet
(1) Försumbar		**Osannolikt** eller **mycket sällan**	< 0,05 ggr/år
(2) Måttlig		**Liten sannolikt** eller **sällan**	0,05-0,5 ggr/år
(3) Betydande		**Stor sannolikhet** eller **regelbundet**	0,5–1 ggr/år
(4) Allvarligt		**Mycket stor sannolikhet eller ofta**	1–10 ggr/år

Konsekvens. Ta del av exempel på specifika konsekvensnivåer i riskanalysens mall för värdering och beskriv konsekvensen kortfattat.

Sannolikhet är ett mått som beskriver hur ofta man skattar att en händelse kommer att inträffa. Det finns flera olika sätt att svara på frågan hur troligt ett specifikt riskscenario är. Ett vanligt sätt är att använda sannolikheter eller frekvenser.

4.1 För in värdet för sannolikhet och konsekvens i riskbedömningen.

4.2 Bestäm vilka risker som ska vidare till steg 3.

5 Steg 3 - Riskhantering.

5.1 Bedöm vilken säkerhetsåtgärd som kan införas för att eliminera eller reducera risken. Beakta eventuella nuvarande skydd. Exempel på lämpliga tekniska och organisatoriska säkerhetsåtgärder finns i dokumentet Lathund för nyttjande av digitala samarbetsverktyg och lagringsytor inom ramen för Umeå universitets verksamhet.

5.2 Säkerställ att säkerhetsåtgärder realiseras.

10. Kompletterande information och slutsats

Om relevant, komplettera i riskanalysmallen, under fliken Komplettering, frågeställningarna nedan.

Tänk på att Dataskyddsförordningen ställer krav på att en specifik konsekvensbedömning ska göras om riskanalysen visar att en viss personuppgiftsbehandling bedöms leda till en hög risk för fysiska personers rättigheter och friheter. I sådana fall ska Dataskyddsombudet vid Umeå universitet kontaktas. Detta utesluter inte att i andra fall göra en generell konsekvensbedömning utifrån ett verksamhets-, ekonomiskt-, förtroende- och individperspektiv.

Kommer bakgrundskunskap att föras in i projektet? Föreligger immaterialrätter kopplade till sådan kunskap?
Hur ska resultat hanteras i projektet – finns krav på nyttjande- eller äganderätter till resultat?

Behöver upphandling av system eller tjänster genomföras av systemet/projektet (observera krav ur GDPR och arkivperspektiv på sådan)?

Ange eventuella slutsatser.

UMEÅ UNIVERSITET

Bilaga

Det finns två mallar för att dokumentera klassningsresultat: en för informationsklassning med tillhörande resurs i form av it-system, och en mall för klassning av forskningsprojekt. Nedan visas dessa två som bilder. Mallarna finns publicerade på https://www.aurora.umu.se/stod-och-service/rad-och-riktlinjer/sakerhet/informationssakerhet/

Informationsklassning: [Systemnamn, verksamhetsområde]

Ansvarig: [Systemägare] Datum: [Datum] Version: [Version nr.]

Klassningsdokumentation

Klassning genomförd:		
Klassning genomförd av:	[Deltagare 1] - Analysledare	
	[Deltagare 2]	
	[Deltagare 3]	
	[Deltagare 4]	
	[Deltagare 5]	
	[Deltagare 6]	
	[Deltagare 7]	
	[Deltagare 8]	
	[Deltagare 9]	
	[Deltagare 10]	
Klassningsresultat:	Konfidentialitet	4
	Riktighet	4
	Tillgänglighet	2

Systemöversikt

Systembeskrivning	[Kort beskrivning av systemet och dess uppgift
Systemleverantör	[Leverantörsnamn]
Systemägare	[Namn och befattning]
Informationsägare	[Namn och befattning]
Personuppgiftsansvarig(-a)	Umeå universitet
Förvaltningsledare	[Namn och befattning]
Förvaltningsledare IT	[Namn och befattning]
Interna användare	[Interna roller]
Externa användare	[Externa roller]
Systemdrift	[Funktion, intern och/eller extern]
Systemsupport	[Funktion, intern och/eller extern]
(Input)	[T.ex. inmatning tangentbord, e-post, systemintegrationer]
(Bearbetning)	[T.ex. beräkningar, sammanställningar m.m.]
(Output)	[T.ex. bildskärm, utskrifter, e-post, integrationer]
Integrationer	[Kopplade system och applikationer]
Lagringsytor	[T.ex. databaser och filmappar]
Manuella rutiner	[T.ex. pappersakter, utskrifter]

Varje informationsbehandling ska klassas. Konceptet här är "högst vinner", det vill säga där varje informationsbehandling blir olika klassad så ska det värde som är högst vara det som styr val av säkerhetsåtgärder.

Klassningen kan justeras högre (men ej lägre) om det motiveras t.ex. av ackumulering av uppgifter (ökad volym av samma typ av uppgifter) eller om system som avses att användas är integrerat med andra systems informationsbehandlingar som har högre klassningsresultat.

Informationssäkerhet

Konfidentialitet (K): Vad kan konsekvenserna bli ifall obehöriga får åtkomst till uppgifterna?

Riktighet (R): Vad kan konsekvenserna bli ifall uppgifterna är felaktiga eller inaktuella?

Tillgänglighet (T): Vad kan konsekvenserna bli ifall någon (som är behörig) inte får tillgång till uppgifterna? .

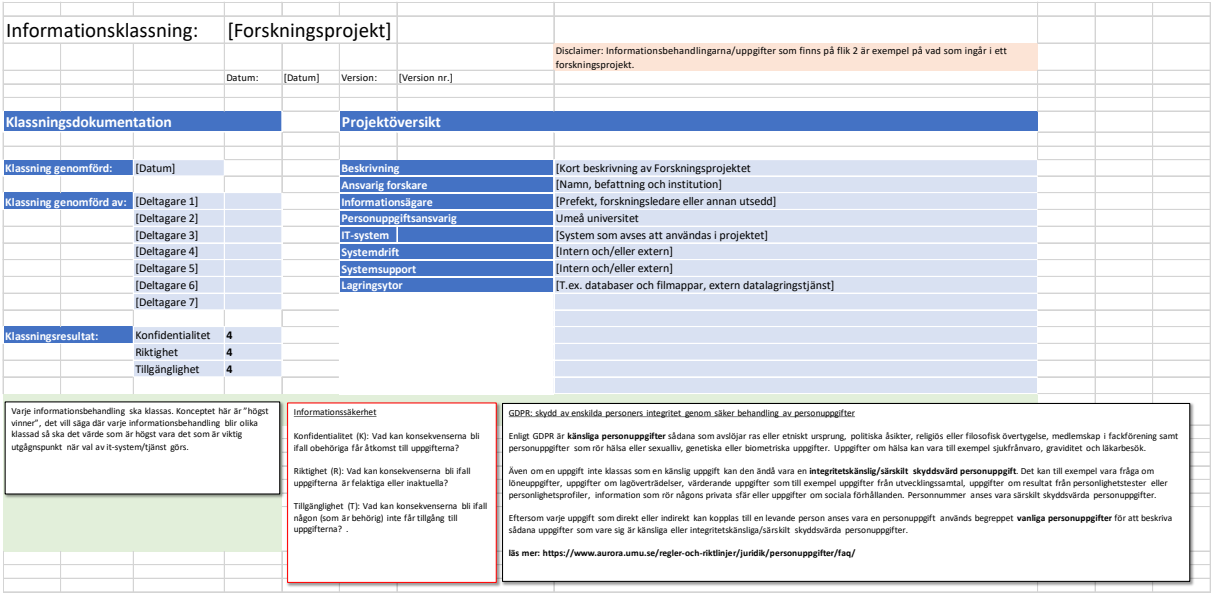
GDPR: skydd av enskilda personers integritet genom säker behandling av personuppgifter

Enligt GDPR är **känsliga personuppgifter** sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv, genetiska eller biometriska uppgifter. Uppgifter om hälsa kan vara till exempel sjukfrånvaro, graviditet och läkarbesök.

Även om en uppgift inte klassas som en känslig uppgift kan den ändå vara en **integritetskänslig/särskilt skyddsvärd personuppgift**. Det kan till exempel vara fråga om löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter som till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler, information som rör någons privata sfär eller uppgifter om sociala förhållanden. Personnummer anses vara särskilt skyddsvärda personuppgifter.

Eftersom varje uppgift som direkt eller indirekt kan kopplas till en levande person anses vara en personuppgift används begreppet **vanliga personuppgifter** för att beskriva sådana uppgifter som vare sig är känsliga eller integritetskänsliga/särskilt skyddsvärda personuppgifter.

läs mer: https://www.aurora.umu.se/regler-och-riktlinjer/juridik/personuppgifter/faq/



Informationsklassning: [Forskningsprojekt]

Disclaimer: Informationsbehandlingarna/uppgifter som finns på flik 2 är exempel på vad som ingår i ett forskningsprojekt.

Datum: [Datum] Version: [Version nr.]

Klassningsdokumentation

Klassning genomförd:	[Datum]	
Klassning genomförd av:	[Deltagare 1]	
	[Deltagare 2]	
	[Deltagare 3]	
	[Deltagare 4]	
	[Deltagare 5]	
	[Deltagare 6]	
	[Deltagare 7]	
Klassningsresultat:	Konfidentialitet	4
	Riktighet	4
	Tillgänglighet	4

Projektöversikt

Beskrivning	[Kort beskrivning av Forskningsprojektet
Ansvarig forskare	[Namn, befattning och institution]
Informationsägare	[Prefekt, forskningsledare eller annan utsedd]
Personuppgiftsansvarig	Umeå universitet
IT-system	[System som avses att användas i projektet]
Systemdrift	[Intern och/eller extern]
Systemsupport	[Intern och/eller extern]
Lagringsytor	[T.ex. databaser och filmappar, extern datalagringstjänst]

Varje informationsbehandling ska klassas. Konceptet här är "högst vinner", det vill säga där varje informationsbehandling blir olika klassad så ska det värde som är högst vara det som är viktig utgångspunkt när val av it-system/tjänst görs.

Informationssäkerhet

Konfidentialitet (K): Vad kan konsekvenserna bli ifall obehöriga får åtkomst till uppgifterna?

Riktighet (R): Vad kan konsekvenserna bli ifall uppgifterna är felaktiga eller inaktuella?

Tillgänglighet (T): Vad kan konsekvenserna bli ifall någon (som är behörig) inte får tillgång till uppgifterna? .

GDPR: skydd av enskilda personers integritet genom säker behandling av personuppgifter

Enligt GDPR är **känsliga personuppgifter** sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening samt personuppgifter som rör hälsa eller sexualliv, genetiska eller biometriska uppgifter. Uppgifter om hälsa kan vara till exempel sjukfrånvaro, graviditet och läkarbesök.

Även om en uppgift inte klassas som en känslig uppgift kan den ändå vara en **integritetskänslig/särskilt skyddsvärd personuppgift**. Det kan till exempel vara fråga om löneuppgifter, uppgifter om lagöverträdelser, värderande uppgifter som till exempel uppgifter från utvecklingssamtal, uppgifter om resultat från personlighetstester eller personlighetsprofiler, information som rör någons privata sfär eller uppgifter om sociala förhållanden. Personnummer anses vara särskilt skyddsvärda personuppgifter.

Eftersom varje uppgift som direkt eller indirekt kan kopplas till en levande person anses vara en personuppgift används begreppet **vanliga personuppgifter** för att beskriva sådana uppgifter som vare sig är känsliga eller integritetskänsliga/särskilt skyddsvärda personuppgifter.

läs mer: https://www.aurora.umu.se/regler-och-riktlinjer/juridik/personuppgifter/faq/

++Exempel på informationstillgångar: