Konsekvensbedömning avseende dataskydd

|  |
| --- |
| **Högskolan i Borås kommentarer:**Dataskyddsförordningen ställer krav på att all behandling av personuppgifter som kan leda till en hög risk för fysiska personers rättigheter och friheter föregås av en bedömning av behand­lingens konsekvenser för skyddet av personuppgifter, en så kallad konsekvens­bedömning avseende dataskydd. I egenskap av personuppgiftsansvarig är högskolan skyldig att utföra konsekvens­bedömning. Om inte annat har beslutats ansvarar chef med verksamhetsansvar för den verksamhet inom vilken behandlingen ska ske för att konsekvensbedömning utförs. Praktiskt kan konsekvensbedömningen dock utföras av andra personer. Konsekvensbedömning är en process för att dokumentera behandlingen av person­uppgifter, identifiera vilka risker som finns med behandlingen, ta fram rutiner och åtgärder för att bemöta dessa risker samt visa att högskolan uppfyller dataskydds­förordningens krav. Konsekvensbedömning ska göras innan behandlingen inleds (kravet omfattar dock även behandling som redan pågår). Påbörja arbetet så fort det är praktiskt möjligt. Genom att använda konsekvensbedömning som ett verktyg i planeringen blir det lättare att fatta rätt beslut i frågor som är viktiga ur ett integritetsperspektiv.Tänk på att konsekvensbedömning är en pågående process som behöver uppdateras och omprövas löpande. Det är därför viktigt att se till att konsekvens­bedömningen är aktuell och att åtgärderna för att hantera riskerna med behandlingen fortfarande är effektiva ifall behandlingen, omständigheter eller risker förändras. Vid frågor om konsekvensbedömning är du välkommen att kontakta högskolans dataskyddsgrupp via e-post, dataskydd@hb.se.  |

**Innehåll**

[1 Allmänt om behandlingen 3](#_Toc83115815)

[2 Bedömning av behovet av konsekvensbedömning 4](#_Toc83115816)

[3 Beskrivning av behandlingen 7](#_Toc83115817)

[4 Åtgärder som bidrar till att behandlingen är proportionell och nödvändig 11](#_Toc83115818)

[5 Åtgärder som stärker de registrerades rättigheter 14](#_Toc83115819)

[6 Hantering av risker för de registrerades rättigheter och friheter 16](#_Toc83115820)

[7 Medverkan från berörda parter 18](#_Toc83115821)

#  Allmänt om behandlingen

## Ansvar m.m.

| Namn på projekt/it-tjänst/behandling/etc. |
| --- |
| Fyll i |
| Ansvarig för personuppgiftsbehandlingen |
| Namn, enhet  |
| Kontaktperson (om annan än ansvarig) |
| Namn, enhet |

## Versionshistorik konsekvensbedömning

| Version | Datum | Fastställd av | Ändringar |
| --- | --- | --- | --- |
| Fyll i | Fyll i | Fyll i | Fyll i |
|  |  |  |  |
|  |  |  |  |

#  Bedömning av behovet av konsekvensbedömning

## Inledning

Det är obligatoriskt att utföra en konsekvensbedömning avseende dataskydd för all behandling av personuppgifter som ”sannolikt leder till en hög risk för fysiska personers rättigheter och friheter”. Som huvudregel föreligger en sådan risk om behandlingen uppfyller två eller fler av kriterierna i punkt 2.2. En behandling kan dock leda till en hög risk även om endast ett, eller inget, kriterium är uppfyllt. Likaså kan det vara möjligt att komma fram till att en behandling inte leder till en hög risk trots att två eller fler kriterier är uppfyllda. I det senare fallet måste skälen till beslutet att inte utföra en konsekvensbedömning dokumenteras.

Exempel på behandlingar som Integritetsskyddsmyndigheten (IMY) anser kräver en konsekvens­bedömning (Förteckning enligt artikel 35.4 i Dataskyddsförordningen, dnr DI-2018-13200):

*Känsliga personuppgifter i forskning*

* Behandling, innefattande lagring i arkiveringssyfte, av pseudonymiserade känsliga person­upp­gifter som rör registrerade från forskningsprojekt eller kliniska prövningar (kriterium 4 och 7).
* Verksamheter som samlar in och lagrar känsliga personuppgifter som ska utgöra underlag för urval för framtida forskningsändamål (kriterium 4 och 7).

*Marknadsföring*

* Ett företag som använder kunders lokaliseringsuppgifter, som till exempel inhämtas via en mobilapp, i syfte att rikta marknadsföring till kunden eller planera sina marknads­förings­strategier (kriterium 3 och 4).
* Ett företag som inhämtar uppgifter från sociala medier för att profilera fysiska personer och därefter rikta marknadsföring till vissa utvalda grupper (kriterium 1 och 3).

*Rekrytering*

* Rekryteringsföretag som inrättar kandidat- eller kompetensdatabaser (kriterium 1 och 4).
* Verksamheter som utför bakgrundskontroller inför rekryteringar (kriterium 1,4 och 6).

*Övrigt*

* En arbetsgivare som övervakar systematiskt hur de anställda använder internet och e-post (kriterium 3 och 7).
* En arbetsgivare som inför ett inpasseringssystem för anställda som innefattar behandling av bio­metriska uppgifter i syfte att identifiera en viss fysisk person, till exempel finger­avtrycks­avläsning (kriterium 3, 7 och 8).
* En organisation inför ett gemensamt system i vilket det är möjligt att anmäla missförhållanden på arbetsplatsen, ett så kallat visselblåsarsystem (kriterium 4 och 7).
* Verksamheter som gör stora ändringar i sin tekniska infrastruktur och som behandlar person­uppgifter inom exempelvis hälso- och sjukvård eller social omsorg (kriterium 4, 7 och 8).

## Bedömning

Den aktuella behandlingen av personuppgifter innebär (välj alla tillämpliga alternativ):

[ ]  Kriterium 1: Utvärdering eller poängsättning, inbegripet profilering eller förutsägelse, särskilt aspekter avseende den registrerades arbetsprestation, ekonomiska situation, hälsa, personliga preferenser eller intressen, pålitlighet eller beteende, vistelseort eller förflyttningar.

[ ] Kriterium 2: Automatiskt beslutsfattande med rättsliga eller liknande betydande följder, det vill säga behandling som har i syfte att fatta beslut som har rättsliga följder för fysiska personer eller på liknande sätt i betydande grad påverkar fysiska personer.

[ ]  Kriterium 3: Systematisk övervakning – behandling som används för att observera, övervaka eller kontroll­era registrerade, inbegripet uppgifter som har samlats in genom nätverk eller systematisk över­vakning av allmän plats.

[ ]  Kriterium 4: Behandling av känsliga personuppgifter enligt artikel 9, personuppgifter som gäller lagöverträdelser enligt artikel 10 samt uppgifter som är av ”mycket personlig karaktär”.

*Känsliga personuppgifter* omfattar etniskt ursprung, politiska åsikter, religiös eller filosofisk över­tygelse, medlemskap i fackförening, genetiska uppgifter, biometriska uppgifter samt uppgifter om hälsa, sexualliv och sexuell läggning. *Personuppgifter om lagöverträdelser* inkluderar uppgifter om brott, domar i brottmål, straffprocessuella tvångsmedel och administrativa frihetsberövanden (till exempel häktning, reseförbud och beslag). *Uppgifter av mycket personlig karaktär* innefattar bl.a. upp­gifter om hushållet och privat verksamhet (såsom elektronisk kommunikation vars konfident­ialitet ska skyddas), eller eftersom de påverkar utövandet av en grundläggande rättighet (såsom lokaliseringsuppgifter vars insamling medför att den fria rörligheten ifrågasätts) eller eftersom åsidosättandet av dessa rättigheter entydigt får allvarliga konsekvenser för den registrerades dagliga liv (till exempel finansiella uppgifter som kan användas för betalningsbedrägeri). Detta kriterium kan även omfatta uppgifter såsom personliga dokument, e-postmeddelanden, dagböcker, kommentarer från läsplattor som är utrustade med kommentarfunktioner och mycket personlig information i applikationer som registrerar aktiviteter.

[ ]  Kriterium 5: Behandling av personuppgifter i stor omfattning med hänsyn till i) antal registrerade som berörs, antingen som ett särskilt antal eller som en andel av den aktuella populationen, ii) mängden uppgifter och/eller variationen av hanterade dataelement, iii) databehandlingens varaktighet eller beständighet samt iv) dess geografiska omfattning.

[ ]  Kriterium 6: Matchande eller kombinerande av personuppgifter från två eller fler behandlingar på ett sätt som avviker från vad de registrerade rimligen hade kunnat förvänta sig, till exempel samkörning av register.

[ ]  Kriterium 7: Behandling av uppgifter om personer som av något skäl befinner sig i ett under­­läge eller i beroendeställning och därför är sårbara, till exempel barn, anställda, asyl­sökande, äldre och patienter.

[ ]  Kriterium 8: Innovativ användning eller tillämpning av nya tekniska och/eller org­anisatoriska lös­ningar, till exempel kombination av fingeravtryck och ansiktsigenkänning för förbättrad fysisk åtkomst­kontroll, eller sakernas internet-applikationer (Internet of things, IoT).

[ ]  Kriterium 9: Behandling av personuppgifter i syfte att hindra registrerade från att få tillgång till en tjänst eller att ingå ett avtal, till exempel bakgrundskontroller i samband med rekrytering.

Kommentar

| Fyll i eventuell förtydligande kommentar |
| --- |

# Beskrivning av behandlingen

## Kategorier av registrerade

Beskriv vilka kategorier av personer som omfattas av behandlingen, deras geografiska hemvist (till exempel Västra Götaland, andra delar av Sverige eller andra länder) och ungefär hur många som berörs. Ange särskilt om barn, äldre, patienter eller andra särskilt sårbara individer berörs.

| Fyll i |
| --- |

## Kategorier av personuppgifter

Beskriv vilka typer av personuppgifter som omfattas av behandlingen (till exempel namn, e-post, röst, bild) och uppskatta hur många uppgifter som behandlas. Se även punkt 3.3-4.

| Fyll i |
| --- |

## Kategorier av känsliga personuppgifter

Ange i förekommande fall vilka typer av känsliga personuppgifter som omfattas av behandlingen och uppskatta hur många uppgifter som behandlas.

| [ ]  Hälsa | [ ]  Genetiska uppgifter | [ ]  Sexualliv eller sexuell läggning |
| --- | --- | --- |
| [ ]  Politiska åsikter | [ ]  Biometriska uppgifter | [ ]  Religiös eller filosofisk övertygelse |
| [ ]  Etniskt ursprung | [ ]  Medlemskap i fackförening |  |

Kommentar:

| Fyll i eventuell förtydligande kommentar |
| --- |

## Kategorier av extra skyddsvärda personuppgifter

Ange i förekommande fall vilka typer av extra skyddsvärda personuppgifter som omfattas av behandlingen och uppskatta hur många uppgifter som behandlas.

| [ ]  Personnummer | [ ]  Lagöverträdelser | [ ]  Personliga egenskaper |
| --- | --- | --- |
| [ ]  Skyddade personuppgifter | [ ]  Sociala förhållanden | [ ]  Lokaliseringsuppgifter |
| [ ]  Sekretessbelagda uppgifter | [ ]  Finansiella uppgifter | [ ]  Internetbeteende o dyl.  |
| [ ]  Övriga uppgifter som ligger nära den privata sfären |  |  |

Kommentar:

| Fyll i eventuell förtydligande kommentar |
| --- |

## Beskrivning av datainsamling

Beskriv hur personuppgifterna kommer att samlas in (metod) och varifrån de kommer (källa), till exempel webbenkät, inspelade intervjuer med de registrerade eller anhöriga, patientjournaler från sjukvården, mikrodata från SCB.

| Fyll i |
| --- |

## Beskrivning av vilken behandling som utförs (funktionell beskrivning)

Förklara steg för steg hur personuppgifterna kommer att användas i praktiken, från insamling till arkivering och gallring. Till exempel lagras, samköras med andra datakällor, transkriberas, pseudo­nymiseras, sammanställas, analyseras, delas med andra, publiceras.

| Fyll i |
| --- |

## Behandlingens ändamål

Förklara vad vill du uppnå med behandlingen av *personuppgifterna*

| Fyll i |
| --- |

## Behandlingens sammanhang

Beskriv behandlingens sammanhang. Till exempel om behandlingen är ny, kontroversiell eller det finns en tidigare problematik med liknande behandlingar eller andra frågor som bör beaktas.

| Fyll i |
| --- |

## Nödvändiga informationstillgångar

Beskriv vilka informationstillgångar som behövs för att genomföra personuppgiftsbehandlingen, till exempel hårdvara, programvara, molntjänster, personer, papper.

| Fyll i |
| --- |

## Lagringsplatser, arkivering och gallring

Ange lagringsplats(er) för de olika typer av information som behandlas och huruvida informationen ska bevaras eller gallras (inklusive gallringsfrist). Vilka handlingar som ska bevaras och gallras regleras i högskolans informationshanteringsplan. Tänk på att ta hänsyn till all lagring, inklusive mellan­lagring eller tillfällig lagring och arkivering.

| **Informationstyp (t.ex. inspelning)** | **Personuppgifter (kategorier)** | **Lagringsplats** | **Bevaras/gallras** |
| --- | --- | --- | --- |
| Fyll i | Fyll i | Fyll i | Fyll i |
|  |  |  |  |
|  |  |  |  |

## Externa mottagare (organisationer och personer utanför högskolan)

Ange i förekommande fall vilka externa mottagare som kommer att få del av person­uppgifterna på något sätt. Till exempel kan det handla om uppgiftsutbyte mellan projektmedlemmar från olika organisationer, överföring av uppgifter till andra myndigheter, publicering av uppgifter i tidskrifter eller på webben för allmänheten.

| **Informationstyp (t.ex. inspelning)** | **Personuppgifter (kategorier)** | **Syfte med överföring** | **Mottagare (t.ex. forskare vid GU)** |
| --- | --- | --- | --- |
| Fyll i | Fyll i | Fyll i | Fyll i |
|  |  |  |  |
|  |  |  |  |

# Åtgärder som bidrar till att behandlingen är proportionell och nödvändig

## Laglig grund för behandlingen

All behandling av personuppgifter måste vara laglig i betydelsen att någon av de lagliga grunder som räknas upp i artikel 6 i dataskyddsförordningen är tillämplig. För ytterligare information, se <https://go.nanolearning.com/LessonViewer/?da=1228235&key=PjnsZiDemZolhNmX&mode=1>

Välj **ett** av alternativen nedan:

[ ]  Alternativ 1: Den registrerade har lämnat samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål (artikel 6.1a dataskyddsförordningen).

[ ]  Alternativ 2: Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås (artikel 6.1b dataskyddsförordningen).

[ ]  Alternativ 3: Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige (artikel 6.1c dataskyddsförordningen).

[ ]  Alternativ 4: Behandlingen är nödvändig för att skydda intressen av grundläggande betydelse för den registrerade eller för en annan fysisk person (artikel 6.1d dataskyddsförordningen).

[ ]  Alternativ 5: Behandlingen är nödvändig för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning (artikel 6.1e dataskyddsförordningen).

Vid alternativ 3 ovan, ange tillämplig bestämmelse i lag eller annan författning.

| Fyll i |
| --- |

## Laglig grund för behandling av känsliga personuppgifter

Som huvudregel är det förbjudet att behandla känsliga personuppgifter. För att få behandla sådana uppgifter måste något av undantagen i artikel 9.1 vara tillämpligt. För ytterligare information, se: <https://go.nanolearning.com/LessonViewer/?da=1228242&key=dxVdVdieSBjrCmrT&mode=1>

Välj **ett** av alternativen nedan (endast om känsliga personuppgifter behandlas):

[ ]  Alternativ 1: Den registrerade har uttryckligen lämnat samtycke till behandlingen av känsliga personuppgifter för ett eller flera specifika ändamål (artikel 9.2a dataskydds­förordningen).

[ ]  Alternativ 2: Behandlingen är nödvändig för att den personuppgiftsansvarige eller registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd (artikel 9.2b dataskyddsförordningen, 3 kap. 2 § data­skyddslagen).

[ ]  Alternativ 3: Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade (artikel 9.2e dataskyddsförordningen).

[ ]  Alternativ 4: Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse (artikel 9.2g dataskyddsförordningen, 3 kap. 3 § data­skydds­lagen).

[ ]  Alternativ 5: Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diag­noser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system (artikel 9.2h dataskydds­förordningen, 3 kap. 5 § dataskyddslagen).

[ ]  Alternativ 6: Behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 (artikel 9.2j dataskyddsförordningen 3 kap. 6 § data­skydds­lagen).

## Nödvändighetskravet

Förklara varför behandlingen är nödvändig för att uppnå det specificerade ändamålet i avsnitt 3. Om det finns andra sätt att uppnå samma ändamål, motivera valet av tillvägagångssätt. Det kan till exempel finnas andra tekniska lösningar eller vara möjligt att använda anonyma, färre eller mindre känsliga uppgifter.

| Fyll i |
| --- |

## Ändamålsbegränsning

Beskriv vilka tekniska och organisatoriska åtgärder som planeras för att förhindra att person­upp­gifterna behandlas för andra, otillåtna, ändamål. Till exempel åtkomstkontroll, instruktioner och utbildning.

| Fyll i |
| --- |

## Uppgiftsminimering

Beskriv vilka tekniska och organisatoriska åtgärder som planeras för att säkerställa att person­upp­­gifterna är adekvata, relevanta och inte för omfattande i relation till ändamålet. Till exempel adekvat utformning av frågeformulär, borttagning av fritextfält och utbildning av den personal som ska samla in uppgifterna.

| Fyll i |
| --- |

## Lagringsminimering

Beskriv vilka tekniska och organisatoriska åtgärder som planeras för att säkerställa att person­uppgifterna bevaras och gallras korrekt (jfr avsnitt 3). Till exempel teknisk funktion för automatisk gallring, meddela leverantören om gallringstider och etablera rutiner för manuell gallring.

| Fyll i |
| --- |

#  Åtgärder som stärker de registrerades rättigheter

## Information till de registrerade

Beskriv när och hur de registrerade kommer att få information om behandlingen. Till exempel i samband med insamling av personuppgifter via e-post, information på webben eller informations­brev vid inhämtande av samtycke.

| Fyll i |
| --- |

## Rätt till tillgång (registerutdrag)

Beskriv hur de registrerades rätt att få information om behandlingen och en kopia av sina person­uppgifter tillgodoses. Normalt behöver det finnas både en teknisk möjlighet att söka fram person­uppgifterna och en rutin för hur en begäran ska handläggas.

| Fyll i |
| --- |

## Rätt till rättelse och radering

Beskriv hur de registrerades rätt att, i vissa fall och alltid efter en prövning, få sina personuppgifter raderade tillgodoses. Normalt behöver det finnas både en teknisk möjlighet att söka fram och gallra person­uppgifterna samt en rutin för hur en begäran ska handläggas.

| Fyll i |
| --- |

## Rätt att göra invändningar och till begränsning av behandling

Beskriv hur de registrerades rätt att invända mot behandlingen och, i vissa fall efter prövning, få behandlingen begränsad tillgodoses. Normalt behöver det både finnas en teknisk möjlighet att sätta uppgifterna i ”karantän” (till exempel att göra uppgifterna otillgängliga för användare eller avpublicera dem från webben tills vidare) samt en rutin för hur en begäran ska handläggas.

| Fyll i |
| --- |

## Personuppgiftsbiträden

Förteckna i tillämpliga fall de personuppgiftsbiträden som anlitas. För ytterligare information, se <https://www.hb.se/anstalld/for-mitt-arbete/informationshantering/behandling-av-personuppgifter-gdpr/allman-information/personuppgiftsansvarig-och-personuppgiftsbitrade/>

| **Biträde(namn)** | **Bistår med följande** | **Behandling sker i (land)** | **PUB-avtal (dnr)** |
| --- | --- | --- | --- |
| Fyll i | Fyll i | Fyll i | Fyll i |
|  |  |  |  |
|  |  |  |  |

## Skyddsåtgärder för internationella överföringar

Som huvudregel är det förbjudet att överföra personuppgifter utanför EU/EES. För att få göra det måste något av undantagen till förbjudet i artikel 44-49 vara tillämpligt. För mer information, se: <https://www.hb.se/anstalld/for-mitt-arbete/informationshantering/behandling-av-personuppgifter-gdpr/allman-information/forbud-mot-overforing-av-personuppgifter-till-tredje-land/>

Förteckna i tillämpliga fall överföringar av personuppgifter till land utanför EU/EES. Ta hänsyn till alla överföringar, inklusive till personuppgiftsbiträden:

| **Mottagare(namn)** | **Syfte med överföring** | **Behandling sker i (land)** | **Laglig grund (artikel 44-49)** |
| --- | --- | --- | --- |
| Fyll i | Fyll i | Fyll i | Fyll i |
|  |  |  |  |
|  |  |  |  |

#  Hantering av risker för de registrerades rättigheter och friheter

## Inledning

Identifiera riskerna för i) obehörig åtkomst, ii) oönskad ändring och iii) förlust av personuppgifter samt övriga relevanta risker med personuppgiftsbehandlingen. Bedöm sannolikheten för att det oönskade ska inträffa och graden av allvar i de konsekvenser som kan uppstå för *de registrerade*.

Gradering av sannolikhet

1 = Osannolikt, men kan hända 2 = Kan förekomma, men endast i sällsynta fall eller i undantagsfall 3 = Möjligt och sannolikt att det skulle uppstå någon gång 4 = Sannolikt att det inträffar ofta 5 = Nästan säkert att det inträffar i de flesta fall

Gradering av konsekvens

1 = Obetydlig 2 = Försumbar 3 = Kännbar 4 = Stor konsekvens 5 = Katastrofal

## Riskbedömning

| **#** | **Beskrivning av riskkälla (oönskad händelse) och möjliga konsekvenserna för de registrerade**  | **Sannolikhet** | **Konsekvens** | **Total risk** |
| --- | --- | --- | --- | --- |
| 1 | Personuppgifter skickas via e-post, med följden att obehörig kan ta del av uppgifterna (felskick, avlyssning, m.m.).  |  |  |  |
| 2 | Personuppgifter lagras på flyttbart lagringsmedia (laptop, mobil, surfplatta, etc.) som förloras eller stjäls, med följden att obehörig kan ta del av uppgifterna.  |  |  |  |
| 3 | Det är oklart vilka som behöver ta del av personuppgifterna med följden att obehörig kan ta del av uppgifterna. Exempel |  |  |  |
| 4 | Personal tar del av personuppgifter som de har behörighet men inte befogenhet att ta del av, med följden att obehörig kan ta del av uppgifterna. |  |  |  |
| 5 | Det saknas rutiner och instruktioner för hur personuppgift­erna ska behandlas, med följden att uppgifterna behandlas felaktigt t.ex. för otillåtna ändamål, att de inte skyddas till­räckligt eller att de inte gallras i tid.  |  |  |  |
| 6 | Personuppgifter överförs till land utanför EU/EES i strid med dataskyddsförordningen, med följden att registrerade går miste om det skydd som garanteras i förordningen eller att deras uppgifter lämnas ut till obehöriga.  |  | 5 |  |
| 7 | Personal har inte genomfört högskolans utbildningar inom dataskydd, informationssäker­het, arkivering och gallring samt offentlighet och sekretess. |  |  |  |

## Åtgärder för att eliminera eller reducera riskerna

Identifiera åtgärder för att eliminera eller reducera identifierade risker (reducera=minska sannolikheten eller begränsa konsekvenserna av risken). Bedöm resterande risk.

| **#** | **Beskrivning av åtgärder för att eliminera eller begränsa risken**  | **Effekt på risk** | **Resterande total risk** |
| --- | --- | --- | --- |
| 1 | Personuppgifter skickas inte via e-post. Istället används xxx för att utbyta information.  | Eliminerar risken |  |
| 2 | Personuppgifter lagras inte på flyttbart lagringsmedia annat än i undantagsfall och då tillfälligt och i krypterad form.Exempel | Reducerar risken |  |
| 3 | Samtliga mottagare (i vissa fall kategorier av mottagare) av personuppgifterna har identifierats. | Reducerar risken |  |
| 4 | Anpassa behörigheter till användarnas roller och behov av information. Etablera rutiner för tilldelning och borttagning av åtkomst och behörigheter. | Reducerar risken |  |
| 5 | Etablera rutiner och instruktioner där det bedöms viktigt och informera personal om dessa.  | Reducerar risken |  |
| 6 | Använda it-tjänster och verktyg som godkänts av högskolan. Informera personal om förbudet mot överföring av per­son­uppgifter till tredjeland.  | Reducerar risken |  |
| 7 | Utbilda personal (högskolans webbutbildningar) | Reducerar risken |  |

## Sammanfattning av risker

Med hänsyn till behandlingen, riskerna med behandlingen och planerade åtgärder för att eliminera eller reducera dessa risker, bedöms den aktuella personuppgiftsbehandlingen inte leda till en hög risk för fysiska personers rättigheter och friheter: [ ]  Ja [ ]  Nej (riktvärde för hög risk => 10)

*I det fall det kvarstår en hög risk för fysiska personers rättigheter och friheter är högskolan skyldig att begära förhandssamråd med Integritetsskyddsmyndigheten innan personuppgiftsbehandlingen får påbörjas. Till exempel kan det handla om att det inte finns några åtgärder för att eliminera eller reducera riskerna eller att de planerade åtgärderna inte begränsar riskerna tillräckligt.*

#  Medverkan från berörda parter

## Samråd med dataskyddsombud enligt artikel 35.2

Enligt artikel 35.2 i dataskyddsförordningen ska högskolans dataskyddsombud alltid rådfrågas vid genom­förande av konsekvensbedömning avseende dataskydd. Ange huruvida dataskydds­ombudet har rådfrågats och sammanfatta dataskyddsombudets synpunkter (bifoga ev. yttrande).

| Fyll i |
| --- |

## Samråd med de registrerade enligt artikel 35.9 (i tillämpliga fall)

Enligt artikel 35.9 i dataskyddsförordningen ska, när det är lämpligt, synpunkter inhämtas från de registrerade eller deras företrädare om behandlingen. Ange huruvida synpunkter har inhämtats och sammanfatta de registrerades synpunkter (bifoga ev. yttrande).

|  Fyll i |
| --- |