Regler för behandling av personuppgifter

Styrdokument	
Rubrik	Regler för behandling av personuppgifter
Klassificering	Regel
Ärendenummer	Ö 308/2018
Beslutsfattare	Rektor
Dokumentansvarig	C HS
Senaste beslutsdatum	2018-05-22
Giltighetstid	Gäller fr o m 2018-05-25 och tillsvidare, dock längst t o m 2018-12-31
Dokument som ersätts	--
Kortare sammanfattning	Reglerna beskriver vad som avses med personuppgifter och regler för hantering av sådana uppgifter.

Regler för behandling av personuppgifter

2. Syfte och mål

Syftet med detta dokument är att beskriva hur Försvarshögskolan, nedan FHS, hanterar personuppgifter. Målet är att vi, genom att följa dessa regler, säkerställer en laglig behandling av personuppgifter som överensstämmer vid var tid gällande dataskyddslagstiftning.

Dessa gemensamma regler gäller för samtliga medarbetare vid FHS som behandlar personuppgifter inom ramen för FHS verksamhet.

3. Behandling av personuppgifter

Den 25 maj 2018 ersatte EU:s dataskyddsförordning (General Data Protection Regulation, GDPR) EU:s dataskyddsdirektiv och därmed även personuppgiftslagen.[1] Dataskyddsförordningen gäller som lag i EU:s medlemsländer men medger och förutsätter nationella särregler på vissa områden. I Sverige finns sådana särregler bl a i lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning (dataskyddslagen) samt i förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning.

3.1 Behandling av personuppgifter

Dataskyddsförordningen gäller för behandling av personuppgifter som är helt eller delvis automatiserade eller annan behandling än automatisk behandling om personuppgifterna ingår eller kommer att ingå i ett register. *(Artikel 1).*[2]

Urval av definitioner *(artikel 4)*

Personuppgift: Uppgift som kan hänföras, direkt eller indirekt, till en fysisk person t ex namn, personnummer, fotografi, onlineidentifikation eller biometriska uppgifter. Uppgifter som är krypterade kan utgöra personuppgifter så länge krypteringsnycklarna finns kvar.

Behandling: Åtgärd eller kombination av åtgärder beträffande personuppgifter t ex insamling, registrering, lagring, bearbetning, överföring eller radering.

Register: En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionell eller geografiska förhållanden.

Personuppgiftsansvarig: Fysisk eller juridisk person, myndighet eller annan organisation som ensamt eller tillsammans med andra bestämmer ändamålet och

---

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EU (allmänna dataskyddsförordningen).
[2] Hänvisning till artikel i dataskyddsförordningen.

medlen för behandlingen av personuppgifter. Det är myndigheten FHS som är ytterst personuppgiftsansvarig, inte den enskilda medarbetaren.

Personuppgiftsbiträde: En fysisk eller juridisk person, myndighet eller annan organisation som behandlar personuppgifter för personuppgiftsansvariges räkning, t ex montjänstleverantörer eller IT-support.

Samtycke: Ett frivilligt, specifikt, informerat och otvetydigt samtycke till behandlingen. Samtycket kan vara uttalat eller entydig bekräftande handling. Den registrerade ska ha fått tydlig information om vilka uppgifter som samlas in och vad syftet är. Personuppgiftsansvarige ska i efterhand kunna visa att ett informerat samtycke har inhämtats.

Ett samtycke ska kunna återkallas av den registrerade. Samtycke som laglig grund för behandlingen ska åberopas när ingen annan laglig grund (se 3.4.) är tillämplig.

3.2 Dataskyddsombud

Enligt dataskyddsförordningen ska den personuppgiftsansvarige i vissa fall utse ett dataskyddsombud. Vid myndigheter och offentliga organ ska det finnas ett dataskyddsombud. Ombudet ska bl a kontrollera att dataskyddsförordningen efterlevs inom organisationen samt utbilda och informera om dataskydd. *(Artiklarna 37-39 och 1 kap 8 § dataskyddslagen)*

3.3 Principer för behandling

Alla medarbetare ska utifrån sitt ansvarsområde verka för att behandla personuppgifter med omsorg och respekt, oavsett om behandlingen rör studenter, medarbetare, leverantörer eller andra registrerade. I arbetet med detta ska alla medarbetare följa de principer för behandling av personuppgifter som ställs upp i dataskyddsförordningen. *Samtliga* principer nedan ska vara uppfyllda vid behandling av personuppgifter. Den personuppgiftsansvarige ska kunna visa att principerna efterlevs *(ansvarsskyldighet). (Artikel 5)*

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt *(laglighet, korrekthet och öppenhet).*
b) Uppgifterna samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna får inte behandlas för ändamål som är oförenligt med det ursprungliga ändamålet *(ändamålsbegränsning).*
c) Uppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålet med behandlingen *(uppgiftsminimering).*
d) Uppgifterna ska vara riktiga och, om nödvändigt, uppdaterade. Felaktiga eller ofullständiga uppgifter ska rättas, blockeras eller utplånas *(korrekthet).*

e) Uppgifterna får bevaras endast så länge det är nödvändigt med hänsyn till ändamålet med behandlingen *(lagningsminimering).*

f) Vid behandling ska lämpliga tekniska eller organisatoriska säkerhetsåtgärder vidtas för satt skydda uppgifterna samt för att förhindra obehörigt intrång eller obehörig behandling, förlust eller annan skada av uppgifterna *(integritet och konfidentialitet).*

Från principerna b och e får göras undantag för behandlingar som avser arkivändamål av allmänt intresse, vetenskaplig eller historiskt forskningsändamål eller statistiska ändamål i enlighet med dataskyddsförordningen.

3.4 Laglig grund för behandling

För varje personuppgiftsbehandling måste det fastställas en laglig grund. *Minst en* av de nedan räknade grunderna ska alltid vara uppfylld vid behandling av personuppgifter. *(Artikel 6)*

- Den registrerade har lämnat sitt samtycke till ett eller flera specifika ändamål.

Behandlingen är vidare tillåten om den är *nödvändig* för att den personuppgiftsansvarige ska kunna

- fullgöra ett avtal med den registrerade,
- fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige,
- skydda grundläggande intressen för den registrerade eller annan person,
- utföra en uppgift av allmänt intresse, eller
- utföra en uppgift som ett led i myndighetsutövningen.

För att kunna åberopa rättslig förpliktelse eller allmänt intresse som laglig grund för behandling, ska den rättsliga förpliktelsen eller allmänna intresset framgå av lag eller annan författning, av kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Som exempel kan nämnas utbildning och forskning som anses vara av uppgifter av allmänt intresse. Lagligt stöd för att en högskola ska behandla personuppgifter i utbildning och forskning finns i 1 kap 2 § högskolelagen där det stadgas att utbildning och forskning är högskolans uppgifter.

Personuppgifter får behandlas som ett led i myndighetsövningen som den personuppgiftsansvarige utövar enligt lag eller annan författning.

Myndigheter kan inte längre åberopa intresseavvägning som laglig grund för behandlingen.

Dataskyddsombudet ska konsulteras vid fastställande av laglig grund.

3.5 Känsliga personuppgifter

Med känsliga personuppgifter (eller så kallad särskild kategori av personuppgifter) avses uppgifter som avslöjar (*Artikel 9)*

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i fackförening,
- genetiska eller biometriska data, samt
- uppgifter om hälsa eller
- uppgift om en fysisk persons sexualliv eller sexuella läggning.

Även indirekta uppgifter kan i vissa fall omfattas av begreppet känsliga uppgifter. T ex kan uppgift om modersmål eller medborgarskap avslöja etniskt ursprung, uppgift om medlemskap i politiskt parti avslöja politiska åsikter eller val av kost (t ex koscher) avslöja religiös övertygelse. Uppgifter om rehabilitering, behov av hjälpmedel (t ex rullstol) eller uppgift om att en student behöver särskilt stöd (t ex ljudinspelning av föreläsningar) kan vara uppgifter om hälsa.

Känsliga personuppgifter har ett särskilt skyddsvärde och det är enligt dataskyddsförordningen förbjudet att behandla känsliga personuppgifter. Det finns dock vissa undantag från förbudet då det är tillåtet att behandla uppgifterna. Vid behandling ska försiktighet iakttas och lämpliga åtgärder vidtas för att skydda uppgifterna.

Nedan några fall då det är tillåtet att behandla känsliga personuppgifter. Ytterliga fall då det är tillåtet att behandla känsliga personuppgifter finns i artikel 9 dataskyddsförordningen och 3 kap 1-7 §§ dataskyddslagen.

- Den registrerade har lämnat *uttryckligt* samtycke till behandlingen eller
- på ett tydligt sätt har offentliggjort uppgifterna,
- behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna fullgöra sina skyldigheter och utöva sina rättigheter inom arbetsrätten eller
- behandlingen är nödvändig för att kunna fastställa eller göra gällande rättsliga anspråk samt
- för att skydda den registrerades eller någon annan persons grundläggande intressen och personen är förhindrad att lämna samtycke.

3.6 Personnummer
Personnummer och samordningsnummer får behandlas utan samtycke endast när det är klart motiverat med hänsyn till

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

Personuppgifter och samordningsnummer anses vara extra skyddsvärda uppgifter och ska behandlas restriktivt. Vid behandling ska lämpliga åtgärder vidtas för att skydda uppgifterna. *(Artikel samt 87 samt 3 kap 10-11 §§ dataskyddslagen)*

3.7 Uppgifter om lagöverträdelser
Med lagöverträdelser avses personuppgifter som rör fällande domar i brottmål och överträdelser. Även misstanke om brott kan i vissa fall omfattas av begreppet lagöverträdelse (t ex om en övervakningskamera fångar en person som begår en lagöverträdelse). Uppgifterna får behandlas av myndigheter. Om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv, får dock även andra än myndigheter behandla uppgifterna. Regeringen eller Datainspektionen får meddela föreskrifter som tillåter att även andra än myndigheter får behandla sådana uppgifter.

Uppgifter om lagöverträdelser anses särskilt skyddsvärda och lämpliga åtgärder ska vidtas för att skydda uppgifterna. *(Artikel 10 samt 3 kap 8-9 §§ dataskyddslagen)*

3.8 Integritetskänsliga uppgifter
Det finns ytterligare en kategori uppgifter som inte är reglerade i lag men som anses vara integritetskänsliga personuppgifter. Det är uppgifter som kan sägas ligga mellan harmlösa och känsliga personuppgifter. Det är uppgifter som för en enskild individ kan verka besvärande om uppgifterna blir kända mer än nödvändigt. Det kan röra sig om uppgifter som omfattas av sekretess eller tystnadsplikt, ekonomiska förhållanden eller annat som ligger nära privatlivet. Dessa uppgifter anses vara skyddsvärda och ska behandlas med försiktighet och med stöd av lämpliga åtgärder för att skydda uppgifterna.

4. Ansvarig handläggare för behandlingen
Det är myndigheten FHS som är personuppgiftsansvarig och ytterst är det styrelsen. Men för att personuppgifter ska behandlas korrekt, ska det för varje behandling utses en ansvarig handläggare.

Den som är ansvarig handläggaren bör ansvara för följande:

- Att behandlingen är förenlig med de principer som anges under 3.3,
- att behandlingen uppfyller minst en av de lagliga grunderna som anges under 3.4,
- att, när det gäller känsliga personuppgifter, personnummer och lagöverträdelser, behandlingen är förenlig med de grunder som anges i 3.5, 3.6 och 3.7 samt med övriga bestämmelser i dataskyddsförordningen, dataskyddslagen och, i förekommande fall, övriga föreskrifter på området.
- att personuppgifter gallras i de fall dem får gallras (vissa uppgifter ska sparas i enlighet med t ex arkivföreskrifter),
- vidta lämpliga åtgärder för skydda uppgifterna med hänsyn till uppgifternas art och behov av skydd,
- att en konsekvensbedömning blir gjord om det är nödvändigt,
- säkerställa att samtycken inhämtas vid behov,
- att uppgifterna behandlas med lämplig säkerhet.

Vid behandling kan/ska dataskyddsombudet rådfrågas. Arbetsuppgifterna kan delegeras ut men ansvarig handläggare kan aldrig frånsäga sig ansvar.

5. Nya behandlingar eller större förändringar

Inför nya behandlingar, eller vid större förändringar i befintliga behandlingar, finns ett antal punkter att särskilt ha i åtanke. Dessa innefattar att avgöra nödvändigheten i personuppgiftsbehandlingen, att överväga risker för den registrerades rättigheter och friheter samt fastställande av laglig grund.

5.1 Nödvändighet

Den första frågan att ställa är vilka personuppgifter som är nödvändiga för att uppfylla ett visst syfte samt att behandlingen uppfyller de grundläggande principerna för personuppgiftsbehandlingar. Kan man uppnå samma syfte med färre personuppgifter eller till och med utan personuppgifter, är det att föredra.

5.2 Konsekvensbedömning

Om behandlingen kan innebära särskilda risker för de registrerade ska det göras en bedömning av vilka konsekvenser behandlingen kan få och vilka åtgärder som behövs för att minska riskerna. Konsekvensbedömningar för behandling av personuppgifter ska alltid genomföras om känsliga, skyddsvärda eller andra integritetskänsliga personuppgifter behandlas. Därutöver ska konsekvensbedömningar genomföras om behandlingen innefattar automatiserat beslutsfattande, inklusive profilering av registrerade, eller systematisk övervakning på allmän plats. *(Artiklarna 35-36)*

Konsekvensbedömningarna ska genomföras under ledning av dataskyddsombudet och dokumenteras skriftligen. Det slutliga protokollet ska undertecknas av den verksamhetsansvarige samt godkännas av dataskyddsombudet. Om dataskyddsombudet gör bedömningen att så behövs, ska Datainspektionen konsulteras för att se om behandlingen möter principerna och kraven för behandling av känsliga personuppgifter. *(Artiklarna 35-36)*

6. Hantering av den registrerades rättigheter

Vid behandling av personuppgifter ska FHS ge klar och tydlig information om personuppgiftbehandlingen och göra allt inom rimlighetens gränser för att bemöta de registrerades behov och rättigheter på ett bra sätt.

6.1 Rätten till information

I samband med att FHS samlar in personuppgifter ska FHS lämna information till den registrerade angående behandlingen. Informationen ska vara klar och tydlig och får inte innehålla svårbegriplig text. FHS har upprättat standardiserade informationstexter för detta ändamål som upprättats i enlighet med de krav som ställs i dataskyddsförordningen. Informationen omfattar bland annat vilka behandlingar som genomförs, ändamålen och laglig grund för behandlingen, information om personuppgiftsansvariga och personuppgiftsbiträden, kontaktuppgifter till dataskyddsombudet samt den registrerades rättigheter. *(Artiklarna 13-14 och 5 kap 1-3 dataskyddslagen)*

Dataskyddsombudet ansvarar för att dessa informationstexter ses över och i förekommande fall uppdateras inför nya behandlingar eller större förändringar i befintliga behandlingar. Dataskyddsombudet ska konsulteras för kvalitetssäkring av dokumenten innan de publiceras.

I normalfallet ska medarbetaren som har den huvudsakliga kontakten med den sökande till utbildning, studenten, den anställde, leverantör eller annan som vänder sig till FHS, lämna ut relevant information om den personuppgiftsbehandling som kommer genomföras. Till exempel har chef HR/chef ansvar för att information lämnas i samband med ingående av anställningsavtal och upphandlingsansvarig ansvarar för att lämna information till leverantör innan kontaktuppgifter för företagets anställda börjar behandlas.

Informationen ska också finnas lättillgänglig i lämpliga digitala kanaler, exempelvis på FHS hemsida, på FHS intranät samt i appar och social media där personuppgifter behandlas.

6.2 Registerutdrag

En som är registrerad har rätt att vända sig till den personuppgiftsansvarige för att få reda på om den personuppgiftsansvarige behandlar uppgifter om den registrerade. Ansökan om s.k. registerutdrag får ske en gång om året och vara undertecknad av antingen den registrerade själv eller av ett ombud med giltig fullmakt. Information om eventuella behandlingar ska normalt lämnas till den registrerade inom en månad och vara kostnadsfritt.

Information som lämnas ska vara skriftligt och ange vilka uppgifter om den registrerade som behandlas, varifrån uppgifterna är hämtade, ändamålen med behandlingen och till vilka mottagare eller kategorier av mottagare som uppgifterna har lämnas ut. *(Artikel 15)*

6.3 Den registrerades övriga rättigheter

FHS är mån om att de registrerades personuppgifter är korrekta. Om en registrerad kontaktar oss angående personuppgifter som de uppfattar som felaktiga eller ofullständiga ska vi rätta, begränsa eller komplettera uppgifterna utan dröjsmål. I tillämpliga fall kan den registrerade ha rätt att få sina personuppgifter raderade, t.ex. om personuppgifterna inte längre är nödvändiga för de ändamål för vilka de samlades in. *(Artiklarna 18-19)*

Om en registrerad invänder mot vår behandling ska en juridisk bedömning göras av behandlingen. I många fall har FHS som myndighet en rättslig skyldighet att behandla personuppgifterna.

I vissa fall har den registrerade även rätt att få ut och överföra sina personuppgifter till annan personuppgiftsansvarig (dataportabilitet). Denna rättighet är kopplad till behandling som avser en tjänst som tillhandahålls av organisationen och som utgår från avtal eller samtycke som rättslig grund. *(Artikel 20)*

Den registrerade har rätt att lämna klagomål avseende behandlingen till FHS dataskyddsombud eller till Datainspektionen (eller annan behörig tillsynsmyndighet inom EU). Den registrerade kan skicka sitt klagomål till dataskyddsombudet. Kontaktuppgifterna till dataskyddsombudet finns på FHS hemsida.

7. Skyldigheter för personuppgiftsansvariga

För varje personuppgiftsbehandling ska det fastställas vilken avdelning eller funktion som är ansvarig handläggare för behandlingen och vilka personuppgiftsbiträden som anlitas. FHS kan vara ensamt personuppgiftsansvarig, gemensamt personuppgiftsansvarig med annan part eller personuppgiftsbiträde åt annan personuppgiftsansvarig. Vem som har vilken roll för olika behandlingar inom organisationen framgår av registerförteckningen.

7.1 Säkerhet
”Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.” *(Artikel 24.1)*

7.2 Inbyggt dataskydd (s.k. Privacy by Design)
Varje personuppgiftsbehandling ska omfattas av lämpliga tekniska och organisatoriska skyddsåtgärder. Vidare ska system och processer vara utformade så att dataskyddsprinciperna (exempelvis uppgiftsminimering) följs. *(Artikel 25)*

För stödsystem som upphandlas via FHS ska kravlistan integreras med inbyggt dataskydd. Avdelningar som upphandlar system är själva ansvariga för att säkerställa att kraven på inbyggt dataskydd är uppfyllda.

7.3. Dataskydd som standard (s.k. Privacy by Default)
Vid varje personuppgiftsbehandling ska den ansvarige för behandlingen se till personuppgifter i standardfallet endast behandlar uppgifter som är nödvändiga för det specifika ändamålet behandlas. Det kan till exempel handla om att de förvalda inställningarna i en tjänst för social media är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas eller behörighetsbegränsningar. *(Artikel 25)*

8. Personuppgiftsbiträden
I de fall då FHS överlåter förvaltningen av personuppgifter till en extern part måste ett personuppgiftsbiträdesavtal upprättas som bilaga till tjänsteavtalet. Personuppgiftsbiträdesavtalet är främst till för att reglera föremålet för behandlingen (exempelvis typen av personuppgifter och kategorier av registrerade), behandlingens varaktighet, art och ändamål samt partnernas skyldigheter och rättigheter. Avtalet ska säkerställa att personuppgiftsbiträdet inte gör saker med de personuppgifter denne förvaltar som står i strid med den personuppgiftsansvariges intentioner.

Även vid anlitande av biträden är det FHS som är personuppgiftsansvarig för behandling av uppgifterna. Innan ett biträde anlitas, ska det säkerställas att biträdet kan garantera att uppgifterna behandlas enligt gällande dataskyddsbestämmelser och att den registrerades rättigheter skyddas.

Den som upphandlar en tjänst som innefattar delning av personuppgifter har ansvaret för att upprätta tillhörande personuppgiftsbiträdesavtal där skyldigheter för personuppgiftsansvariga och personuppgiftsbiträden regleras. *(Artikel 28-29)* Vid upprättanande av ett biträdesavtal ska dataskyddsombudet och/eller högskolans jurister rådfrågas.

8.1 Underbiträde

Ibland anlitar personuppgiftsbiträdet ett eller flera underbiträden. Detta ska i förekommande fall regleras i avtalet. Personuppgiftsbiträdet ansvarar för underbiträden så som för sig själv. Biträdet får inte föra över uppgifter till underbiträde utan FHS godkännande. Biträdet ska redovisa för FHS vilka underbiträden som anlitas. *(Artikel 28.2)*

9. Register över personuppgiftsbehandlingar

Varje avdelning inom organisationen ska föra register över sin behandling. I första hand är det ansvarige handläggaren som ska föra register över sina behandlingar. Dataskyddsombudet har ansvaret för att ha en förteckning över samtliga behandlingar som görs vid FHS. *(Artikel 30)*

Anlitas biträden, ska även dessa föra register över de behandlingar som genomförs för FHS räkning. *(Artikel 30.2)*

10. Utlämnande av information till tredje part

Delning av personuppgifter till tredje part (inklusive familjemedlem) ska vanligtvis inte ske. I undantagsfall kan sådant utlämnade bli aktuellt till exempelvis polismyndighet eller annan myndighet.

I samband med t ex verksamhetsövergång kan personuppgifter vara en av de tillgångar som förs över till en ny personuppgiftsansvarig. Om ändamålet med personuppgiftsbehandlingen hos den nya personuppgiftsansvarige är detsamma som hos den tidigare, är en sådan överföring tillåten. För att de registrerade ska kunna tillvarata sina rättigheter även efter övergången måste den övertagande personuppgiftsansvarige informera de registrerade om vem som är ny personuppgiftsansvarig.

Dataskyddsombudet ska konsulteras i samband med delning av personuppgifter till tredje part för att säkerställa att detta är lagligt samt att överföringen genomförs på ett korrekt sätt.

11. Överföring av personuppgifter utanför EU/EES

Inom EU och EES-området säkerställer dataskyddsförordningen att den registrerade får ett likvärdigt skydd för sina personuppgifter. Utanför EU och EES-området (s.k. tredjeland) finns dock inte motsvarande garantier. I de fall vi vill överföra personuppgifter utanför EU/EES ska vi använda oss av särskilda avtalsklausuler (standardavtalsklausuler) upprättade av EU-kommissionen, med den som mottar uppgifterna i tredjeland. Om uppgifterna inom en koncern förs till ett bolag i tredjeland, kan bindande företagsbestämmelser (Binding Corporate Rules) användas.

Undantag finns för ett fåtal länder som EU-kommissionen anser uppfyller kraven för en adekvat säkerhetsnivå för överföring av personuppgifter. Listan över länder som EU-kommissionen ”godkänt” finns på Datainspektionens hemsida. Likaså har EU och USA skapat ett ramverk för kontroll av adekvat säkerhetsnivå, den s.k. privatlivsskölden (Privacy Shield). För närvarande har ett tusental amerikanska företag anslutit sig till privatlivsskölden och är därmed ”godkända” för överföring av personuppgifter. För dessa överföringar räcker ”ett vanligt” personuppgiftsbiträdesavtal. Listan över företag i USA som är anslutna till Privacy Shield finns på det amerikanska handelsministeriets webbplats.

I de fall överföring till tredjeland inte kan ske med stöd av adekvata skyddsnivåer, standardavtalsklausuler, privatsköldar eller andra likvärdiga beslut, får överföring ske i vissa undantagsfall och med de restriktioner som finns i artikel 49. Överföring kan t ex vara tillåten om den är nödvändig och det föreligger ett uttryckligt samtycke eller för att överföringen är nödvändig för fullgöra ett avtal eller är viktig av skäl som rör allmänintresset. Ytterligare några fall då överföring är tillåten finns i dataskyddsförordningen. *(Artiklarna 44 -50)*

Dataskyddsombudet ska konsulteras inför överföring av personuppgifter utanför EU/EES till länder och/eller organisationer som inte uppfyller EU-kommissionens krav på säker överföring eller som inte är anslutna till privatlivsskölden.

12. Personuppgiftsincidenter

All misstänkt, obehörig eller otillbörlig behandling av personuppgifter ska rapporteras som en personuppgiftsincident till dataskyddsombudets särskilda e-postadress så snart det upptäcks. Detta gäller oavsett om FHS agerar som personuppgiftsansvarig eller personuppgiftsbiträde.

Personuppgiftsincidenter som medför en risk för fysiska personers rättigheter och friheter ska rapporteras till tillsynsmyndigheten utan dröjsmål, maximalt 72 timmar efter att de kommit till FHS kännedom. Om incidenten sannolikt leder till hög risk för de registrerade ska även dessa informeras utan dröjsmål.

Ansvarig verksamhetschef ska, med stöd av dataskyddsombudet tillse att det finns tillfredställande processer för identifiering av personuppgiftsincidenter och att samtliga personuppgiftsbiträden är skyldiga att anmäla personuppgiftsincidenter till ansvarig handläggare för behandlingen inom organisationen utan dröjsmål.

Dataskyddsombudet ansvarar för att bedöma om incidenten ska rapporteras till tillsynsmyndigheten. Dataskyddsombudet är också ansvarigt för att det finns tillfredställande processer för hantering av personuppgiftsincidenter.
(Artiklarna 33-34)

Vid FHS finns en tjänst i IT-portalen där information finns om incidentrapportering.

13. Hantering av personuppgifter i särskilda situationer

I detta stycke beskrivs hur personuppgifter ska hanteras i ett antal särskilda situationer

13.1 Ostrukturerad information

Med ”ostrukturerad information” menas *”vardaglig ostrukturerad behandling av personuppgifter som löpande text i ordbehandlingssystem, löpande text på internet, ljud- och bildupptagningar och korrespondens per e-post.”* samt *”enkla strukturer som klasslistor och listor över anställda”* – om materialet inte ingår i eller ska infogas i en databas med en personuppgiftsanknuten struktur, till exempel ett ärendehanteringssystem.

Detta innebär generellt att medarbetare måste vidta samma försiktighet i hantering av personuppgifter i mejl, dokument i filservers, sociala medier, excel-listor och liknande som de gör i centrala IT-system.

Behandling av personuppgifter i ostrukturerat format ska i möjligaste mån undvikas. I den mån det ändå sker är samtliga medarbetare ansvariga för att (minst) årligen rensa och radera personuppgifter i ostrukturerat format. För detta ändamål har FHS infört en årlig rensardag **(”Stora Rensardagen”)** där de anställda uppmanas att sätta av tid för att rensa och radera bland ostrukturerad information. Vidare har samtliga medarbetare ett ansvar för att hitta mer beständiga alternativ vid ”systematisk hantering av ostrukturerad information” där informationen exempelvis lagras på säkra ytor och delas via länkar till informationen snarare än att informationen skickas i mejl.

Ansvariga för IT-system som hanterar personuppgifter i ostrukturerat format (exempelvis CRM-system samt system för ärende- och incidenthantering) ska tillse att fritextfält endast används där det är absolut nödvändigt och att de i förekommande fall säkerställer att personal som arbetar i systemen utbildas på vad som är acceptabelt kontra icke acceptabelt att skriva i fritextfält. Detta för att minimera risken att kränkande eller olämpliga personuppgifter och omdömen lagras.

Medarbetare ska informeras om sitt ansvar för hantering av ostrukturerad information samt vad de får och inte får göra i de etiska riktlinjerna samt särskilda dokument som beskriver tillåten hantering av FHS IT-resurser. Dataskyddsombudet ska tillsammans med ansvariga för informationssäkerheten säkerställa att medarbetarna utbildas i hanteringen av ostrukturerad information samt att de årligen påminns om sitt ansvar.

13.2 Publicering på nätet

Myndigheter ska enligt 6 § myndighetsförordningen informera om sin verksamhet. Information om verksamheten anses vara en uppgift av allmänt intresse och den lagliga grunden för att behandling av uppgifterna (som ibland kan innehålla personuppgifter) på hemsidan, finns således i myndighetsförordningen. Givetvis gäller dataskyddsförordningen även för att detta och ibland behövs det samtycket (t ex vid publicering av bilder från mingel el dyl) för att kunna publicera informationen.

Vidare ska grundläggande krav på behandlingen vara uppfyllda såsom att FHS informerar de registrerade på ett korrekt sätt samt för register över vår behandling. För att säkerställa att personuppgiftsbehandlingen på webben eller i löpande text sker korrekt ska all sådan publicering hanteras av kommunikationsavdelningen.

13.3 Studenternas behandling av personuppgifter

FHS är ansvarig för personuppgiftsbehandlingar som förekommer i studenternas arbeten i utbildningsverksamheten. Personuppgiftsbehandling inom utbildning ska följa de riktlinjer och rekommendationer, med avseende på exempelvis beskrivning av ändamål, laglig grund och hur de registrerade informeras. Avsteg från dessa riktlinjer och rekommendationer ska dokumenteras och godkännas av rektor.

13.4 Kamerabevakning

Det åvilar säkerhetschefen för organisationen att tillse att lämpliga rutiner finns för korrekt och lagenlig behandling av kamerabevakning. Innan sådan användning sker bör dataskyddsombudet rådfrågas.

13.5 Barns personuppgifter

Vårdnadshavare har inte automatiskt rätt att utöva den registrerades rättigheter för sina barns räkning utan de registrerade barnens medgivande. Detta eftersom barn är egna individer som har rättigheter och friheter enligt dataskyddsförordningen. Om FHS har medarbetare som är 16 år och uppåt, ska medarbetardata inte lämnas ut till vårdnadshavare utan den registrerade medarbetarens medgivande.

13.6 Samarbetspartners

Externa parter ska som utgångspunkt inte ha tillgång till personuppgifter där FHS är personuppgiftsansvarigt. Extern part anses då vara en så kallad tredje part, vilket i normalfallet kräver samtycke från student, anställd eller någon annan registrerad, vid överföring av personuppgifterna. För det fall extern part ska få tillgång till personuppgifter ska detta skriftligen regleras.

Varje samarbetspartner är personuppgiftsansvarig för de uppgifter som behandlas (samlas in, används, lagras, delas etc.) och varje samarbetspartner har därför skyldighet att säkerställa att dataskyddsförordningen följs.

13.7 Skyddad identitet

Hantering av personuppgifter för person med skyddad identitet kräver särskild hänsyn. FHS ska säkerställa ändamålsenliga rutiner för medarbetare i sådant avseende.

14. Radering av personuppgifter

Personuppgifter får endast sparas, det vill säga förvaras i en form som möjliggör identifiering av den registrerade, under så lång tid som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. När personuppgifterna inte längre behövs för dessa ändamål ska de raderas eller avidentifieras. För att säkerställa att personuppgifter inte sparas längre än nödvändigt, har FHS upprättat rutiner för gallring.

Observera att FHS som myndighet har en skyldighet att bevara vissa uppgifter enligt arkivbestämmelser eller bestämmelser i andra författningar. I vissa fall kan uppgifterna gallras efter några år och i vissa falla bevaras uppgifterna för alltid. Information om bevarandetider finns i dokumentationshanteringshanteringsplaner för forskning och utveckling. Dokumenthanteringsplaner för övriga handlingar kommer att utarbetas.

15. Testdata

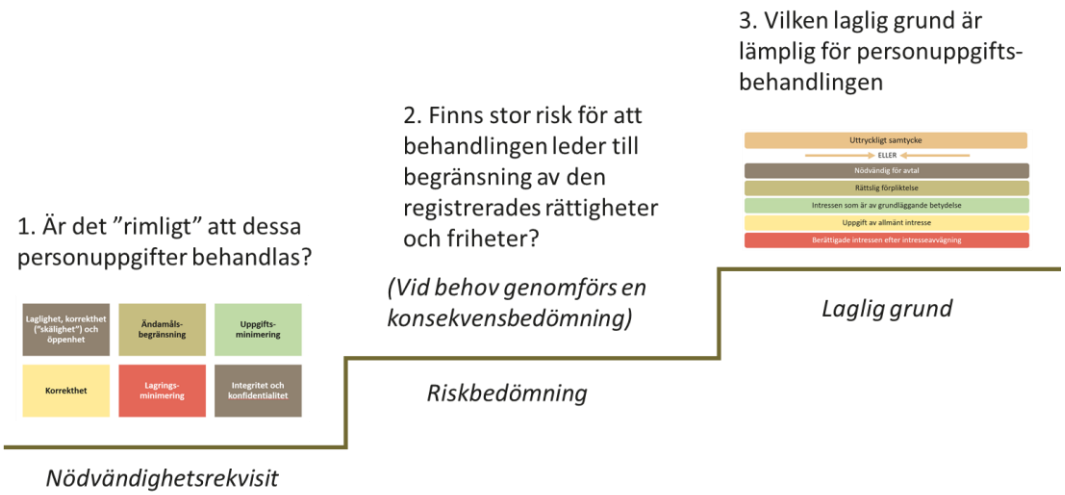
Organisationen ska, så långt det är möjligt, använda fingerade eller avidentifierade personuppgifter vid tester. Testmiljö och produktionsmiljö bör vara tydligt åtskilda och det ska finnas rutiner på plats som förhindrar att testpersonal av misstag utför åtgärder i produktionsmiljön.

I de situationer personuppgifter används i testmiljön gäller samma regler som i produktionsmiljön. Detta innebär att instruktioner till användare, behörighetsstyrning, loggning och IT-säkerhet ska behandlas lika i testmiljön som i produktionsmiljö.

16. Policys, rutiner etc

Mera detaljerade bestämmelser eller rutiner för dataskyddsarbetet vid FHS finns i de policys, rutiner och annat som utarbetas inom området. De finns tillgängliga på FHS intranät. Information om behandlingar som vänder sig till studenter och allmän finns på FHS hemsida.

Att tänka på innan man påbörjar en behandling



* Myndigheter kan inte åberopa intresse avvägning som laglig grund för behandling.