Regler för anställdas behandling av personuppgifter vid Högskolan i Borås

Målgrupp för styrdokumentet	Anställda
Publicerad	Högskolans styrdokument
Typ av styrdokument	Regel
Beslutsfattare	Rektor
Beslutsstöd	5 kap. 5 § styrelsens organisations- och beslutsordning (SOB)
Beslutsdatum	2018-06-18
Giltighetstid samt revideringsperiodicitet	Tillsvidare, följs upp 1 gång per år eller vid behov
Ansvarig funktion	Kommunikation
Version	1

Sammanfattning

Dessa regler gäller hur anställda får behandla personuppgifter i arbetet.

Syftet med reglerna är att säkerställa att behandling av personuppgifter sker enhetligt och korrekt, och att informera om hur sådan behandling följs upp.

Innehållsförteckning

INLEDNING

Bakgrund

Rätt till privatliv och skydd av personuppgifter är två grundläggande rättigheter. En korrekt behandling av personuppgifter är därför viktig och ett krav inom hela Högskolan i Borås verksamhet. En felaktig behandling av personuppgifter kan skada enskilda, och leda till sanktionsavgifter, skadestånd och förtroendeskada för högskolan.

Syfte

Dessa regler riktar sig till samtliga anställda, oavsett anställningsform, som behandlar personuppgifter i arbetet. Detta inbegriper även externa ledamöter, sakkunniga och andra externa personer som behandlar personuppgifter under högskolans ledning.

Behandling av personuppgifter regleras av flera författningar, bl.a. dataskyddsförordningen och dataskyddslagen. På vissa områden finns det särskilda författningar som etikprövningslagen inom forskning, och patientdatalagen och socialtjänstens föreskrifter inom studenthälsan. Därtill har författningar som förvaltningslagen, offentlighets- och sekretesslagen, och arkivlagen också betydelse för hur personuppgifter får behandlas. Tillsynsmyndighetens riktlinjer och beslut har stor betydelse i sammanhanget. Sammantaget är regelverket kring behandling av personuppgifter svåröverskådligt och komplicerat, vilket kan göra det svårt att bedöma hur personuppgifter får behandlas.

Syftet med dessa regler är att säkerställa att den grundläggande behandlingen av personuppgifter sker enhetligt och korrekt, samt informera om hur denna behandling följs upp.

Läsanvisningar

Samtliga anställda: s. 1-18, 23-25

Forskare: s. 1-18, 20-23, 23-25

Lärare: s. 1-18, 18-19, 23-25

VIKTIGA BEGREPP

Personuppgifter
Med ”personuppgifter” menas alla uppgifter som ensamt, eller i kombination med andra uppgifter, kan knytas till en fysisk person som är i livet.

Kommentar
Exempel på personuppgifter är personnummer, namn, adress, rumsnummer, befattning, telefonnummer, mejladress, elektroniska identiteter av olika slag som användarnamn, ORCID, alias/handles på sociala medier, datornamn, IP-adress, samt bank-, betal-, och kreditkortsnummer, registreringsnummer, passnummer, ärendenummer etc., samt bild- och ljudupptagningar där enskilda individer går att identifiera.

Ofta kan kombinationen av dels en uppgift som är tillgänglig för en själv och som inte är en tydlig personuppgift, dels en uppgift som är tillgänglig för andra personer, betyda att den egna uppgiften är en personuppgift. Exempelvis säger bara ett kreditkortsnummer inget om kortinnehavaren, men då numret går att knyta till en person med hjälp av de uppgifter som banken har tillgång till, är kreditkortsnumret ändå att betrakta som en personuppgift. Det har alltså ingen betydelse vem som har tillgång till den andra uppgiften som gör det möjligt att knyta den egna uppgiften till en person.

Personuppgifter som har krypterats, dvs. förvanskats på så sätt att ingen annan än den som har tillgång till ytterligare information (en så kallad ”kodnyckel”) kan läsa dem är fortfarande att betrakta som personuppgifter.

Uppgifter om aktiebolag och andra juridiska personer som organisationsnummer är inte personuppgifter, eftersom de inte gäller en fysisk person. Motsvarande uppgifter om enskilda näringsidkare (personnummer) är däremot att anse som personuppgifter.

Känsliga personuppgifter
Med ”känsliga personuppgifter” menas alla personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, genetiska uppgifter, biometriska uppgifter, medlemskap i fackförening samt uppgifter om hälsa, sexualliv och sexuell läggning.

Kommentar
Exempel på känsliga personuppgifter är sjukfrånvaro, beskrivningar av sjukdomar eller annan fysisk eller psykisk ohälsa, uppgifter om funktionsvariationer, särskilda behov, allergier och hemland. Uppgifter som indirekt avslöjar känsliga uppgifter, är känsliga personuppgifter. Exempelvis kan matpreferenser avslöja religiös övertygelse.

Extra skyddsvärda personuppgifter
Med ”extra skyddsvärda personuppgifter” menas integritetskänsliga uppgifter.

Kommentar
Det finns ingen definition av vad extra skyddsvärda personuppgifter är i författning utan begreppets innebörd har främst utvecklats i tillsynsmyndighetens praxis. Uppgifter som omfattas av sekretess eller tystnadsplikt, skyddade personuppgifter, uppgifter om lagöverträdelser, vissa uppgifter om ekonomiska förhållanden, samt beskrivningar och värderingar av personliga egenskaper och förhållanden eller förhållanden som annars ligger nära den privata sfären är exempel på uppgifter som tillsynsmyndigheten ansett vara extra skyddsvärda.

Integritetskänsliga personuppgifter
Med ”integritetskänsliga personuppgifter” menas känsliga personuppgifter och extra skyddsvärda personuppgifter. Begreppet används alltså som en samlingsbeteckning för de båda kategorierna av personuppgifter.

Behandling
Med ”behandling” menas alla åtgärder som kan vidtas med personuppgifter elektroniskt, t.ex. registrering, lagring, läsning, sammanställning, samkörning, utskrift av digitala dokument etc., ändring, överföring, spridning och radering.

Den registrerade
Med ”den registrerade” menas den person vars personuppgifter behandlas.

Mottagare
Med ”mottagare” menas den person till vilken personuppgifter lämnas ut.

Personuppgiftsansvarig
Med ”personuppgiftsansvarig” menas den som ensamt eller tillsammans med andra bestämmer över ändamålet och medlen för personuppgiftsbehandlingen.

Kommentar
Normalt är högskolan personuppgiftsansvarig, men vid samverkan med andra lärosäten, myndigheter eller företag kan en av parterna, eller parterna gemensamt, vara personuppgiftsansvarig.

Personuppgiftsbiträde
Med ”personuppgiftsbiträde” menas en fysisk eller juridisk person som behandlar personuppgifter för högskolans, eller en annan personuppgiftsansvarigs, räkning. En leverantör av en molntjänst är exempel på ett personuppgiftsbiträde.

IT-system
Med ”IT-system” menas de IT-system, applikationer, verktyg, tjänster och dylikt som det finns en utsedd systemägare för inom högskolan, med undantag för lagringsytorna/tjänsterna F:, G:, Vibe, och Box.

Systemägare
Med ”systemägare” menas den som har ett dokumenterat ansvar för administration och drift av ett eller flera IT-system, applikationer, verktyg, tjänster och dylikt.

Tredje part
Med ”tredje part” menas någon annan än den registrerade, den personuppgifts-ansvarige, personuppgiftsbiträdet, eller de personer som är behöriga att behandla personuppgifter under den personuppgiftsansvariges eller personuppgiftsbiträdets ledning.

Sociala medier
Med ”sociala medier” menas Facebook, Twitter, LinkedIn, Instagram, Messenger, SnapChat, WhatsApp, YouTube, Vimeo, HB Play, bloggar och liknande tjänster.

Ärende
Med ”ärende” menas mellanhavanden inom högskolan eller mellan högskolan och enskilda som mynnar ut i ett beslut av något slag från högskolans sida. Med beslut menas ett uttalande eller ställningstagande som har någon form av återverkan eller vägledning för en student, anställd eller en annan individ, eller högskolan.

Kommentar
Myndighetsutövning i form av beslut om antagning, dispenser, studieuppehåll/anstånd, omprövning av betyg, examination, utfärdande av examen, disciplinärenden och begäran om att lämna ut allmän handling är alltid att betrakta som beslut, och således ärende.

Till ett ärende hör varje uppgift med betydelse för beslutet, t.ex. korrespondens mellan lärare och student av betydelse för examination, tjänsteanteckningar och beslutsförslag. Tillfälliga noteringar, minnesanteckningar som inte tillför ett ärende sakuppgift, eller kladdlappar, noteringar och dylikt som förlorat sin betydelse i samband med att en handling upprättats är exempel på uppgifter som inte hör till ett ärende.

Ren informationsgivning, t.ex. uppgifter som rör undervisningen eller studiesituationen i stort, som när en föreläsning börjar, vilken litteratur som ska läsas, förtydliganden av vad som sagts på en föreläsning, frågor kring hur man gör för att få studieuppehåll etc. är andra exempel på uppgifter som inte hör till ett ärende.

Det finns inget formkrav på hur ett ärende inleds. Ett ärende kan alltså inledas genom ett mejl, en skrivelse eller ett överklagande etc. till en medarbetare vid högskolan. Det kan också inledas genom eget initiativ inom högskolan.

Tredje land
Med ”tredje land” menas ett land som inte ingår i EU/EES.

GRUNDLÄGGANDE PRINCIPER

Det finns sju grundläggande principer som styr all behandling av personuppgifter. En medvetenhet och förståelse för dessa är viktig för förståelsen av reglerna i följande avsnitt. De är också riktlinjer att falla tillbaka på när det saknas regler för en specifik situation.

1) Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (principen om laglighet, korrekthet och öppenhet).

2) Personuppgifter ska bara behandlas om det är nödvändigt. De får bara samlas in för särskilda, uttryckligt angivna och berättigande ändamål, och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (principen om ändamålsbegränsning).

3) Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till ändamålen med behandlingen (principen om uppgiftsminimering).

4) Personuppgifter ska vara korrekta och om nödvändigt uppdaterade. Personuppgifter som är felaktiga i förhållande till ändamålen med behandlingen ska rättas eller raderas (principen om korrekthet).

5) Personuppgifter ska inte lagras i en form som möjliggör att den registrerade kan identifieras under en längre tid än vad som är nödvändigt för ändamålen med behandlingen (principen om lagringsminimering).

6) Personuppgifter ska behandlas på ett säkert sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling samt mot förlust, förstöring eller skada genom olyckshändelse (principen om integritet och konfidentialitet).

7) Den personuppgiftsansvarige ansvarar för, och ska kunna visa, att dessa principer samt dataskyddslagstiftningens regler följs (principen om ansvarsskyldighet).

Kommentar
Aktuell bestämmelse: Artikel 5 dataskyddsförordningen

De grundläggande principerna är riktlinjer vars närmare innebörd tydliggörs av reglerna i följande avsnitt. Inte desto mindre är en medveten och förståelse för dessa viktig för förståelsen av reglerna eller då regler saknas för en specifik situation.

REGLER FÖR BEHANDLING AV PERSONUPPGIFTER

Allmänt

1 §
Dessa regler gäller anställda och andra som behandlar personuppgifter under högskolans ledning. Studentkårens ledamöter och studentrepresentanter omfattas av reglerna när de medverkar i styrelser och råd samt vid beredning och beslut av ärenden som har betydelse för utbildningen eller studenternas situation. I övrigt omfattas inte studenter av dessa regler.

2 §
a) Chef med verksamhetsansvar ansvarar för att informera sina medarbetare om innehållet i dessa regler.

b) Enskild medarbetare ansvarar för att den egna behandlingen av personuppgifter sker enligt dessa regler.

c) Systemägare ansvarar för tillämpning av dessa regler inom sitt ansvarsområde.

Rättslig grund

Myndighetsutövning, allmänt intresse, rättslig förpliktelse, avtal

3 §
Personuppgifter får behandlas om det är nödvändigt för att fullgöra en uppgift a) som innefattar myndighetsutövning, eller b) vars ändamål är av allmänt intresse, eller c) som följer av lag eller avtal. Vilka ändamål som är av allmänt intresse anges i högskolans register över personuppgiftsbehandlingar.

Kommentar
Aktuell bestämmelse: Artikel 6 dataskyddsförordningen

All insamling, registrering, lagring, spridning och annan behandling av personuppgifter måste vila på rättslig grund. Rättslig grund kan vara att behandlingen av personuppgifter är nödvändig för att fullgöra en uppgift som inbegriper myndighetsutövning eller vars ändamål är av allmänt intresse, eller som följer av lag eller avtal.

Nödvändighetskravet

Gemensamt för dessa rättsliga grunder är att behandlingen av personuppgifter ska vara nödvändig för att kunna fullgöra uppgiften. Det innebär att om ändamålet med uppgiften kan uppnås med rimliga medel utan att personuppgifter behandlas, ska personuppgifter inte behandlas. Det innebär också att personuppgifter som inte är nödvändiga för att uppfylla ändamålet med behandlingen inte ska samlas in, spridas etc.

Det är den som avser att behandla personuppgifter som har att göra en bedömning om behandlingen är nödvändig för att kunna fullgöra uppgiften. Det är viktigt att göra en ordentlig bedömning och kunna motivera den. I det fall tillsynsmyndigheten skulle komma fram till att nödvändighetskravet inte är uppfyllt är behandlingen olaglig. Högskolan kan då bli skadeståndsskyldig mot de vars personuppgifter behandlats felaktigt samt få betala kraftiga sanktionsavgifter till staten.

Nödvändighetskravet gör sig särskilt gällande vid användningen av IT-system som ger möjlighet att skriva text fritt (fritext), eftersom risken är större än annars för att onödiga personuppgifter antecknas. Det är därför viktigt att bedöma vilka personuppgifter som är nödvändiga och se till att endast sådana personuppgifter antecknas eller hämtas in av andra, t.ex. genom enkäter, formulär och intervjuer etc.

Allmänt intresse

Beträffande den rättsliga grunden ”allmänt intresse” ska behandlingen av personuppgifter ha ett tydligt samband med högskolans uppdrag att utbilda, forska, samverka med omgivande samhälle, informera om högskolans verksamhet och verka för att forskningsresultat kommer till nytta. Den närmare innebörden av begreppet allmänt intresse är emellertid inte given. Med hänsyn till detta och svårigheterna att bedöma vad som är av allmänt intresse innehåller högskolans register över personuppgiftsbehandlingar en förteckning över vad som är att betrakta som allmänt intresse.

Rättslig förpliktelse

Beträffande den rättsliga grunden ”rättslig förpliktelse” ska den rättsliga förpliktelsen följa av lag eller annan författning, kollektivavtal eller av beslut som har meddelats med stöd av lag eller annan författning. Den rättsliga förpliktelsen ska också vara så tydlig att den registrerade kan förstå och förutse vilken behandling av personuppgifter som utförs. Exempel på sådana rättsliga förpliktelser finns i förordning (1993:1153) om redovisning av studier m.m. vid universitet och högskolor (”Ladokförordningen”).

Avtal

När det gäller den rättsliga grunden ”avtal” ska behandlingen av personuppgifter framgå av ett avtal med den vars personuppgifter ska behandlas. Den registrerade måste alltså vara avtalspart.

Samtycke

4 §
Personuppgifter får behandlas med samtycke.

Kommentar
Aktuell bestämmelse: 6 § dataskyddsförordningen

Ett samtycke är ett godkännande från den registrerade av en eller flera specifika behandlingar av personuppgifter. Samtycke som rättslig grund är främst aktuellt vid behandling av vissa kategorier av personuppgifter enligt 5 §, eller när de rättsliga grunderna enligt 3 § inte är användbara.

Samtycke kan inte användas i vissa situationer, nämligen då det råder ett ojämlikt förhållande mellan den som vill samla in personuppgifter och den som anmodas lämna samtycke. Det beror på att samtycket i dessa fall inte bedöms vara frivilligt. Förhållandet mellan högskolan och anställda och/eller studenter kan i vissa fall vara ett sådant förhållande. Det är då inte givet att ett samtycke kan betraktas som frivilligt. Om det kan antas att förhållandena är sådana att ett samtycke inte kan lämnas frivilligt bör högskolans dataskyddsfunktion kontaktas för samråd.

5 §
Följande behandling av personuppgifter får endast utföras med samtycke:

a) Publicering av bild- och/eller ljudmaterial som innebär att enskilda individer går att identifiera på webben och sociala medier m.m. (Internet).

   Undantag: Publicering av bild- och/eller ljudmaterial som innehåller personuppgifter på Internet kan undantagsvis få ske med stöd av annan rättslig grund efter godkännande av högskolans dataskyddsfunktion.

b) All behandling av personnummer (8 eller 10 siffror)

   Undantag: Personnummer får behandlas utan den registrerades samtycke om det är klart motiverat med hänsyn till vikten av en säker identifiering av honom eller henne, ändamålet med behandlingen eller något annat beaktansvärt skäl.

c) All behandling av känsliga personuppgifter

   Undantag: Känsliga personuppgifter får behandlas i löpande text om uppgifterna har lämnats i ett ärende av någon utomstående eller om de är nödvändiga för handläggningen av ett ärende.

Undantag: Känsliga personuppgifter som lämnats till högskolan får handläggas och diarieföras enligt reglerna om hur inkomna handlingar ska hanteras, samt i övrigt behandlas om behandlingen är ett direkt krav enligt lag.

Undantag: Känsliga personuppgifter får behandlas om det är nödvändigt för att högskolan eller den registrerade ska kunna utöva och fullgöra sina rättigheter och skyldigheter inom arbetsrätten. Sådana personuppgifter får inte lämnas ut till tredje part, såvitt det inte finns en skyldighet att göra det eller den registrerade uttryckligen samtyckt till utlämnandet.

Undantag: Känsliga personuppgifter får behandlas om det är nödvändigt av ändamål som hör samman med hälso- och sjukvård, och behandlingen sker av en person som omfattas av lagstadgad tystnadsplikt.

Kommentar

Publicering av bild- och ljudmaterial på Internet
Aktuella bestämmelser: HB-regel

Det finns ingen bestämmelse i dataskyddsförordningen eller annan författning som uttryckligen förbjuder publiceringen i fråga. Beroende på bl.a. hur och i vilket sammanhang personen återges, t.ex. fakta-, porträtt-, eller stämningsbild, i vilket sammanhang publicering sker, t.ex. marknadsföring eller reportage, i vilka medier publicering sker, t.ex. tryckta medier, webb eller sociala medier, vilka andra personuppgifter som publiceras tillsammans med bilden, *finns* det en risk för att materialet uppfattas som integritetskänslig.

Webben, och framförallt sociala medier, innebär också vissa särskilda risker. Det som publiceras kan läsas av många och nå en inte önskvärd spridning som inte är möjlig att stoppa. Högskolan kan inte heller säkerställa att Facebook, Instagram, YouTube m.fl. faktiskt raderar material på vår begäran eller hur dessa företag själva använder det material som publiceras.

Till sist är utrymmet för att grunda publiceringen på allmänt intresse mycket begränsat. I samband med t.ex. evenemang av större betydelse eller andra viktigare händelser som vissa utmärkelser, projekt och resultat där man kan räkna med att fotografering eller filmning förekommer, kan allmänt intresse bli aktuellt. Utrymmet är dock begränsat och dessutom krävs det att publiceringen är nödvändig. Med hänsyn till svårigheterna att bedöma om det är möjligt att använda allmänt intresse som rättslig grund krävs därför godkännande av högskolans dataskyddsfunktion till behandlingen. Sådant godkännande kan innehålla villkor, t.ex. att information om förekomsten av fotografering eller filmning ska lämnas på inbjudan till evenemanget eller vid det aktuella tillfället.

I det fall samtycke används bör frågan om att lämna samtycke ges innan fotograferings eller filmningstillfället. Inhämtande av samtycke i situationer som kan innebära att samtycket inte är frivilligt bör undvikas, t.ex. spontana gruppbilder.

Användning av personnummer
Aktuell bestämmelse: 3 kap. 10 § dataskyddslagen

Behandling av personnummer kräver som huvudregel samtycke. Behandling av personnummer får dock ske utan samtycke i vissa fall, främst om det är klart motiverat med hänsyn till vikten av att en person inte ska förväxlas med en annan person. Kravet på att det ska vara klart motiverat är ett högt ställt krav. Det innebär att i första hand ska någon annan identifierare, eller kombination av identifierare, användas, t.ex. signatur, namn, födelsedatum, mejladress etc.

Exempelvis är det många gånger inte motiverat att använda personnummer i kontakt-, deltagar-, och närvarolistor och dylikt, mötesanteckningar, statistiksammanhang eller vid felsökning och support. Om den aktuella personen har ett namn som gör att han eller hon kan förväxlas med en annan person går det oftast bra att använda födelsedatum, mejladress eller signatur istället för personnummer.

Känsliga personuppgifter
Aktuella bestämmelser: Artikel 9 dataskyddsförordningen och 3 kap. 2, 3 och 5 §§ dataskyddslagen

Behandling av känsliga personuppgifter kräver som utgångspunkt samtycke. Till huvudregeln finns det ett antal undantag, bl.a. för handläggning av ärenden samt inom arbetsrättens område och studenthälsan. Gemensamt för dessa undantag är att behandlingen av känsliga personuppgifter ska vara nödvändig, se kommentaren till 3 § för ytterligare information om nödvändighetskravet.

Beträffande undantaget inom arbetsrättens område rörande utlämning av känsliga personuppgifter till tredje part, kan det framhållas att tredje part t.ex. omfattar fackliga organisationer, myndigheter som Försäkringskassan, och företag. Känsliga personuppgifter som uppgift om facktillhörighet eller sjukdom får alltså inte lämnas ut till dessa, eller annan tredje part, med mindre än att det finns samtycke eller en lagstadgad skyldighet.

6 §

Samtycke ska vara skriftligt och hämtas in innan behandlingen av personuppgifter påbörjas. Högskolans mallar för inhämtande av samtycke ska användas.

Kommentar
Aktuell bestämmelse: Artikel 7 dataskyddsförordningen

För att en person ska kunna ta ställning till en förfrågan om samtycke måste denne få information om vad personuppgiftsbehandlingen innebär. Av informationen ska det bl.a. framgå vad ändamålet med behandlingen är, hur uppgifterna kommer att behandlas, hur länge uppgifterna kommer att lagras, vilka rättigheter den registrerade har m.m. Med hänsyn till vikten av att den registrerade får en fullständig information ska högskolans mallar för inhämtade av samtycke användas. Samtycke ska lämnas skriftligt.

7 §

Samtycken ska bevaras och hållas ordnade. Rutin som säkerställer detta ska upprättas i samråd med arkivarie och dokumenteras innan samtycke hämtas in.

Kommentar
Aktuell bestämmelse: Artikel 7 dataskyddsförordningen

Högskolan ska kunna visa att den registrerade har samtyckt till en viss behandling av personuppgifter. Det krävs därför att inhämtade samtycken bevaras och hålls ordnade.

8 §
Behandling av personuppgifter ska ske i enlighet med inhämtat samtycke. Om annan behandling ska ske måste nytt samtycke hämtas in innan behandlingen påbörjas eller annan rättslig grund åberopas.

Kommentar
Aktuell bestämmelse: Artikel 7 dataskyddsförordningen

Ett samtycke ska alltid avse en viss specifik behandling av personuppgifter. I det fall någon annan behandling ska ske måste därför ett nytt samtycke hämtas in som avser den nya behandlingen eller annan rättslig grund åberopas. Nytt samtycke ska hämtas in före den nya behandlingen påbörjas.

9 §
I det fall en registrerad tar tillbaka ett lämnat samtycke ska behandlingen av den registrerades personuppgifter upphöra. Rutin som säkerställer att behandlingen upphör ska upprättas och dokumenteras innan samtycke hämtas in.

Kommentar
Aktuell bestämmelse: Artikel 7 dataskyddsförordningen

När behandling av personuppgifter sker med stöd av samtycke kan den registrerade återkalla lämnat samtycke. Behandlingen av den registrerades personuppgifter måste då upphöra. Det innebär t.ex. att den registrerades personuppgifter inte får publiceras på nytt eller ingå i nya beräkningar, samkörningar, sammanställningar etc. Den behandling som redan skett – och eventuella resultat av den – påverkas emellertid inte.

Informationsskyldighet

10 §
Dessa regler gäller vid behandling av personuppgifter enligt 3 §.

11 §
I samband med insamling av personuppgifter genom blanketter, enkäter, formulär och dylikt eller personlig kontakt, ska information om behandlingen av personuppgifter lämnas till den registrerade.

12 §
Vid insamling av personuppgifter som ska användas för att kommunicera med den registrerade ska information om behandlingen av personuppgifter lämnas vid kommunikation med den registrerade.

13 §
Information om behandlingen av personuppgifter ska lämnas av den som samlar/t in personuppgifterna genom en hänvisning till högskolans integritetspolicy.

Kommentar 10-13 §§
Aktuella bestämmelser: Artikel 12-22 och 34 dataskyddsförordningen

Kravet på att lämna information till den registrerade gäller oavsett om personuppgifterna erhållits av den registrerade själv eller någon annan. Information bör lämnas genom en hänvisning till högskolans integritetspolicy på webben.

Observera att kravet på information gäller i förhållande till alla som högskolan behandlar personuppgifter om. Inom ramen för bl.a. administration och handläggning av ärenden kan det förekomma att personen saken berör lämnar uppgifter om andra personer. Om det är nödvändigt registrera personuppgifter om dessa andra personer ska de också erhålla information om personuppgiftsbehandlingen.

Lagring, arkivering och radering

Lagring

14 §

a) Icke-integritetskänsliga personuppgifter får lagras i godkända och anvisade IT-system, F: och G:, Vibe, Box, samt mobila enheter och flyttbart lagrings-media.

b) Integritetskänsliga personuppgifter får lagras i godkända och anvisade IT-system, F: och G:, samt krypterat flyttbart lagringsmedia. Särskilda regler finns för Ping Pong i 27 §.

c) Samma information innehållande personuppgifter bör inte lagras på flera ställen (så kallad ”dubbellagring”)

d) Personuppgifter får inte föras över till tredje land utan godkännande av högskolans dataskyddsfunktion.

Åtkomst, behörigheter m.m.

15 §

a) Åtkomst till integritetskänsliga personuppgifter ska vara personlig och begränsad till de medarbetare som behöver uppgifterna i sitt arbete.

b) Rutin för tilldelning och borttagning av åtkomst till integritetskänsliga person-uppgifter och som säkerställer att varje medarbetare har rätt behörighetsnivå ska vara dokumenterad och följas.

c) Varje IT-system ska som huvudregel ha ett system för behörighetskontroll som gör det möjligt att kontrollera behörigheten vid åtkomst samt följa upp åtkomstförsök i efterhand. För varje lyckat/misslyckat åtkomstförsök ska det

framgå minst användarnamn, tidpunkt och till vilken information åtkomst har begärts.

d) Rutin för uppföljning av behandlingshistorik (så kallade ”loggar”) ska vara dokumenterad och följas. Av rutinen ska det framgå hur ofta loggarna ska följas upp och analyseras, vem som har ansvar för analysen, hur länge loggarna ska lagras och vart de ska lagras.

16 §

a) Systemägare ansvarar för den tekniska tilldelningen och borttagningen av åtkomst enligt 15 § a) samt tillämpningen av 15 § c-d) inom ramen för sitt ansvarsområde.

b) Chef med verksamhetsansvar ansvarar för tillämpningen av 15 § a) och b) inom sitt ansvarsområde.

Kommentar 14-16 §§
Aktuella bestämmelser: Artikel 5 (principerna om uppgifts- och lagringsminimering samt principen om integritet och konfidentialitet), 24, 32 och 89 dataskyddsförordningen samt tillsynsmyndighetens praxis

Högskolan är ansvarig för att skyddet av personuppgifter alltid är tillräckligt för de personuppgifter som behandlas. Det ställer krav på hur personuppgifter lagras. Mobila enheter som bärbara datorer, telefoner och surfplattor används ofta utanför högskolans lokaler och är stöldbegärlig egendom. Det är svårare att avgöra om användaren av mobila enheter är behörig. Det finns dessutom möjlighet att själv installera appar och program. De kan emellertid oavsiktligt eller avsiktligt sprida personuppgifter som enheten har tillgång till. Mobila enheter medför därför särskilda risker som kan få svåra konsekvenser för både enskilda och högskolan. Möjligheterna att lagra personuppgifter på mobila enheter är därför av säkerhetsskäl begränsad.

Lagring av personuppgifter i andra än godkända och anvisade IT-system och lagringsytor är också begränsad på grund av att högskolan saknar ett så kallat personuppgiftsbiträdesavtal med leverantörer av andra system och tjänster, vilket är ett krav för att det ska vara tillåtet att föra över och lagra personuppgifter hos dessa. Exempelvis är det inte tillåtet att lagra personuppgifter på lagringstjänster som Google Drive, Dropbox, iCloud eller OneDrive. Det är inte heller tillåtet för anställda att lagra sådana uppgifter i molntjänster som G Suite (Google Docs, m.m.).

För integritetskänsliga personuppgifter gäller dessutom högre säkerhetskrav, vilket också begränsar vart personuppgifter får lagras.

Arkivering och radering

17 §

a) Personuppgifter som inte längre är nödvändiga, men som inte får raderas enligt högskolans informationshanteringsplan ska arkiveras.

b) Arkivering ska ske på särskilt anvisat sätt, eller genom att så långt det är möjligt begränsa åtkomsten till informationen som innehåller personuppgifterna till ett fåtal medarbetare i samråd med arkivarie.

c) Information innehållande personuppgifter som inte längre är nödvändiga, och som får raderas enligt högskolans informationshanteringsplan, ska raderas.

d) Rutin för när integritetskänsliga personuppgifter ska arkiveras och raderas ska dokumenteras och följas.

18 §

a) Varje medarbetare ansvarar för tillämpningen av 17 § a-c) avseende den egna mejlen, webbformulär och personliga lagringsutrymmen som hemkatalog, Box och Vibe.

b) Systemägare ansvarar för tillämpningen av 17 § a-d) inom sitt ansvarsområde.

c) Chef med verksamhetsansvar ansvarar för tillämpningen av 17 § a-d) inom sitt ansvarsområde avseende gemensamma lagringsytor som G:, Box och Vibe.

Kommentar 17-18 §§
Aktuella bestämmelser: Artikel 5 dataskyddsförordningen (principerna om uppgifts- och lagringsminimering), 3 och 10 §§ arkivlagen, Riksarkivets föreskrifter i tillämpliga delar samt högskolans informationshanteringsplan

Information är en av högskolans viktigaste tillgångar och får inte tas bort hur som helst. Som myndighet har högskolan också ett ansvar att tillgodose allmänhetens insyn i verksamheten, vilket ställer krav på hur information som innehåller personuppgifter ska arkiveras och raderas.

Nödvändighetskravet

Information som innehåller personuppgifter ska antingen arkiveras eller raderas när den inte längre är nödvändig. Med detta menas att det inte längre finns något befogat behov av informationen i det vardagliga arbetet med hänsyn till ändamålet med behandlingen.

Exempel (alla exempel utgår från att informationen innehåller personuppgifter):

Exempel 1
Enligt högskolans informationshanteringsplan ska information som är, eller förutses bli, en del av ett ärende registreras och lagras i anvisat system enligt högskolans rutin för ärenden, till exempel Diariet (W3D3), Ladok och Nais. Informationen bör därefter tas bort

från alla andra lagringsytor och medier, eftersom det i regel inte finns något befogat behov av att lagra samma information på flera platser (principen om lagringsminimering).

Exempel 2
Enligt högskolans informationshanteringsplan får utkast och annat arbetsmaterial raderas när det slutgiltiga förslaget har upprättats. Arbetsmaterial som minnesanteckningar och dylikt förlorar ofta sin betydelse i samband med att den slutgiltiga versionen av ett beslutsförslag eller en rapport etc. har upprättats. Om så är fallet ska minnesanteckningarna raderas, eftersom informationen förlorat sin betydelse.

Om det efter att den slutgiltiga versionen av ett beslutsförslag etc. har upprättats finns ett behov av minnesanteckningarna i ett annat sammanhang innebär det oftast att det är fråga om en ny behandling av personuppgifter som måste följa aktuella principer och regler. Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål (principen om ändamålsbegränsning).

Exempel 3
Enligt högskolans informationshanteringsplan får administrativa listor av tillfällig betydelse, som inte är en del av ett ärende, raderas vid inaktualitet. Exempel på sådana listor är Excellistor och dylikt för planering, uppföljning, statistik och annan administration av kurser och evenemang, kontakter/intressenter, antagning, stipendier, särskilt stöd till studenter, in/utresande studenter och personal, och VFU. Listor som är en del av att ärende eller som används inom forskning omfattas inte.

Personuppgifter som t.ex. samlats in om deltagare till ett evenemang för att kunna beställa mat finns det i regel inte något befogat behov av efter att maten beställts, varför de ska raderas vid denna tidpunkt. Om uppgifterna däremot dessutom samlats in för att kunna skicka information om liknande evenemang i framtiden är situationen annorlunda. I sådant fall kan det vara rimligt att spara uppgifterna tills personen i fråga meddelar att den inte längre vill ha information. Observera att den registrerade alltid ska informeras om syftet med behandlingen och vid vilken tidpunkt personuppgifterna raderas.

Observera att uppgifter i listor kan användas för olika ändamål och att uppgifter som inte längre är nödvändiga i ett sammanhang fortfarande kan vara nödvändiga i ett annat.

<u>Arkivering</u>
Arkivering kan ske genom att information som innehåller personuppgifter avskiljs från det verksamhetssystem som används i det dagliga arbetet och lagras i ett särskilt arkiv. De som berörs av arkivering på detta sätt får information om detta av arkivarie.

I annat fall ska arkivering ske genom att åtkomst till information som innehåller personuppgifter begränsas till ett fåtal medarbetare. Informationen får då endast användas för arkivändamål i fortsättningen med hjälp av dessa medarbetare.

En lista över när de vanligaste typerna av information får raderas enligt högskolans informationshanteringsplan finns i registret över personuppgiftsbehandlingar.

Kontakta i första hand arkivarie vid frågor om när information får raderas enligt högskolans informationshanteringsplan.

Radering
Med radering menas att personuppgifterna inte går att återskapa. Det kan ske på två sätt. För det första kan personuppgifter raderas genom att informationen innehållande personuppgifter, t.ex. ett Word-dokument, tas bort (”delete”). För det andra kan personuppgifter raderas genom att informationen innehållande personuppgifter avidentifieras. Med detta menas att uppgifter som går att knyta till den registrerade tas bort ur informationen medan andra uppgifter behålls. Under förutsättning att kopplingen till den registrerade bryts och det inte går att hitta tillbaka till den registrerade anses personuppgifterna vara raderade.

Särskilt om mejl och sociala medier

Mejl m.m.

19 §
Information som innehåller personuppgifter får mejlas till de som har ett nödvändigt behov av informationen i sitt arbete.

Kommentar
Aktuell bestämmelse: Artikel 5 dataskyddsförordningen (principerna om uppgifts- och lagringsminimering samt principen om integritet och konfidentialitet)

När det gäller intern mejlkorrespondens är utgångspunkten att man bara ska mejla information som innehåller personuppgifter till de medarbetare som behöver informationen i sitt arbete. Det är därför viktigt att överväga vilka som verkligen behöver informationen, särskilt i fråga om kopiemottagare (”cc”).

Beträffande extern mejlkorrespondens är utgångspunkten densamma, men här får man även observera att det finns förbud mot att skicka känsliga personuppgifter i arbetsrättsliga sammanhang till tredje part, se 4 §. Det kan även finnas andra författningar som reglerar hur personuppgifter får spridas, t.ex. Ladokförordningen.

Observera också att personer kan ha olika behov av information. I fråga om t.ex. planering av ett evenemang kan en medarbete behöva uppgift om deltagarnas namn för att göra namnskyltar till bordsplacering (men inga andra uppgifter om deltagarna), medan en restaurang kan behöva uppgift om allergier, men ofta inga andra uppgifter om deltagarna. Det kan alltså vara nödvändigt att behöva dela upp information beroende på mottagarens behov.

20 §
Information som innehåller personuppgifter bör i första hand delas med andra genom hänvisningar eller länkar till informationen i godkända och anvisade IT-system och lagringsytor.

Kommentar
Aktuell bestämmelse: Artikel 5 dataskyddsförordningen (principerna om uppgifts- och lagringsminimering)

Att dela dokument m.m. som innehåller personuppgifter genom mejl medför att samma information finns på flera ställen. Det medför också problem vid radering av personupp-

gifterna, eftersom mottagaren inte nödvändigtvis känner till när dessa ska raderas. Detta ska undvikas enligt principerna om uppgifts- och lagringsminimering. I första hand ska därför hänvisningar eller länkar till informationen användas. Informationen lagras då på ett ställe, och skaparen av informationen kontrollerar borttagningen av densamma.

Länkar kan t.ex. användas till information som lagras i IT-system som Diariet, eller lagringsytor som G:, Vibe, Box. I det fall det inte är tekniskt möjligt att använda länkar bör man hänvisa till informationen, t.ex. kan man i mejl skriva ”Önskar synpunkter på utkast, vänligen se dokument med namn *abc* i systemet *xyz*”.

I det fall mottagaren inte har åtkomst dit informationen lagras bör man överväga om informationen verkligen är nödvändig för mottagaren. I andra fall bör man lösa det genom lämpliga lagrings/katalog- och behörighetsstrukturer, om möjligt.

21 §

Interna och externa mejl som innehåller integritetskänsliga personuppgifter ska krypteras. I första hand ska det ske med anvisad programvara. I andra hand ska de integritetskänsliga personuppgifterna bifogas som krypterade filer. I det senare fallet ska lösenordet till dokumentet kommuniceras separat.

Kommentar
Aktuell bestämmelse: Artikel 5 (principen om integritet och konfidentialitet), 24 och 32 dataskyddsförordningen samt tillsynsmyndighetens praxis

22 §

a) Skrivelser och korrespondens som är av ringa eller tillfällig betydelse för högskolans verksamhet som enklare frågor, reklam, kursinbjudningar och massutskick, ska raderas när den inte längre är nödvändig.

b) Skrivelser och korrespondens som bedöms leda till ett ärende, eller som är en del av ett ärende, ska registreras och hanteras enligt högskolans rutiner för ärenden i anvisat system. Kopior av skrivelser och korrespondens som arkiverats ska raderas.

c) Arbetsmaterial/utkast ska raderas när det slutgiltiga förslaget är upprättat.

d) Intern korrespondens ska raderas när den inte längre är nödvändig.

   Undantag: Skrivelser och korrespondens som tillför ett ärende en sakuppgift ska hanteras enligt 21 § b).

Kommentar
Aktuella bestämmelser: Artikel 5 dataskyddsförordningen (principen om lagrings-minimering), 3 och 10 §§ arkivlagen, Riksarkivets föreskrifter i tillämpliga delar samt högskolans informationshanteringsplan

Det centrala i dessa regler är begreppen ”ärende” och ”nödvändigt” Se kommentar till 17-18 §§ för en närmare beskrivning av nödvändighetskravet, samt kommentar till ärende-

begreppet under avsnittet ”Viktiga begrepp”. Här kan endast tilläggas att korrespondens som inte är, eller förutses bli, en del av ett ärende i regel bör ha korta raderingsfrister. Mejl ska inte betraktas som ett lagringssystem.

Sociala medier

23 §

a) Varje konto, sida, kanal eller motsvarande på sociala medier med anknytning till arbetet vid högskolan ska godkännas av kommunikationschef.

b) För varje konto, sida, kanal eller motsvarande på sociala medier ska det finnas en dokumenterad rutin för arkivering och radering av personuppgifter.

c) Medarbetare som företräder högskolan i sociala medier ska särskilt iaktta kravet på samtycke enligt 4 § a) samt följa högskolans rutiner för sociala medier.

Kommentar
Aktuell bestämmelse: HB-regel

Sociala medier innebär stora möjligheter att marknadsföra högskolan och kommunicera med studenter och andra intressenter, men också vissa risker. Det som publiceras kan läsas av många och nå en inte önskvärd spridning, som högskolan inte kan stoppa. Högskolans ansvar för sociala medier ställer också särskilda krav på det som publiceras av högskolan, och i vissa fall kontroll m.m. av vad andra externa personer publicerar. Med hänsyn till bl.a. detta är möjligheterna begränsande för enskilda medarbetare att skapa och använda sociala medier i arbetet.

Särskilt om administrativa listor m.m.

Det är vanligt med Excellistor och dylikt av olika slag i administrativa sammanhang. Exempel på sådana listor är listor för planering, uppföljning och annan administration av tjänstgöring/bemanning, semester, arbetsuppgifter, löner, tillbud och arbetsskador, fakturering och/eller betalning, in/utresande studenter och personal, antagning, stipendier, deltagare (kurser etc.), närvaro, examinatorer, projektrapportering, kontaktuppgifter etc. Innehållet i dessa listor är mycket varierande.

Det finns inga särskilda regler för hur listor med personuppgifter ska hanteras, utan det är samma regler som för annan information. Det innebär främst följande:

1) Personuppgifter får behandlas i listor, om behandlingen är nödvändig för att fullgöra en uppgift som innefattar myndighetsutövning eller vars ändamål är av allmänt intresse, eller som följer av lag eller avtal.

2) Listor får endast innehålla sådana personuppgifter som är nödvändiga för att ändamålet med listan kan kunna uppfyllas, se kommentar till 3 och 17-18 §§.

3) Personnummer samt känsliga personuppgifter i listor kräver som utgångspunkt samtycke, se 5 §.

4) Information om personuppgiftsbehandlingen ska lämnas till den registrerade enligt 11-12 §§.

5) Listor ska lagras enligt 14-15 §§, arkiveras och raderas enligt 17-18 och 22 §§, samt mejlas, eller på annat sätt delas med andra, enligt 19-21 §§.

6) Beträffande listor med kontaktuppgifter till externa intressenter som används för att skicka ut information om högskolans organisation och verksamhet gäller följande. Vid kommunikation ska en information lämnas enligt 12-13 §§. Dessutom ska det finnas en tydlig beskrivning av hur man går tillväga för att avanmäla/avregistrera sig från fler utskick. I fråga om mejlutskick som sker genom avdelning kommunikation läggs det till en länk för avregistrering. Kontaktuppgifter till personer som har avanmält/avregistrerat sig ska omedelbart raderas.

Kompletterande regler inom utbildning

24 §
Kursmoment och ämnesval ska som huvudregel utformas på så sätt att studenter inte behöver behandla personuppgifter för att kunna uppnå kursmålen.

I det fall det bedöms viktigt att studenter behandlar personuppgifter för att uppnå kursmålen ska studenterna få klar och tydlig information om hur de ska behandla personuppgifter.

Studenter får inte behandla integritetskänsliga personuppgifter inom utbildning på grundnivå och avancerad nivå.

Kommentar
Aktuell bestämmelse: HB-regel

Högskolan är ansvarig för studenters behandling av personuppgifter inom ramen för sina studier. Det innebär att högskolan vid risk för sanktionsavgifter och skadestånd har att se till att studenter behandlar personuppgifter enligt högskolans beslutade regler.

Med hänsyn till svårigheterna för högskolan att styra och följa upp studenters behandling av personuppgifter enligt beslutade regler bör kursmoment som innefattar personuppgiftsbehandling undvikas. Detta innebär också att i fråga om val av ämne för uppsatser och examensarbeten m.m. ska ämnen som innebär att personuppgifter behandlas undvikas.

Studenter får aldrig behandla integritetskänsliga personuppgifter inom utbildningen. Av förarbetsuttalanden framgår bl.a. att det inte är rimligt att förvänta sig att studenter som genomgår utbildning på grundnivå eller avancerad nivå med säkerhet har hunnit tillägna sig kunskaper och insikter i den omfattning som krävs för att hantera potentiellt integritetskänsliga uppgifter (se prop. 2007/08:44, s. 20). Detta medför också att sådana uppgifter inte får lagras i Ping Pong.

I det fall det anses nödvändigt att studenter behandlar personuppgifter ska behandlingen ske med samtycke. Studenters personuppgiftsbehandling kräver alltså alltid samtycke från den vars personuppgifter ska behandlas. Observera därvid att ett samtycke alltid kan återkallas, varvid personuppgifterna inte får användas mer.

25 §

I det fall studenter har att behandla personuppgifter, ansvarar kursansvarig för att studenterna får klar och tydlig information om hur studenterna ska behandla personuppgifter enligt högskolans beslutade regler.

Kursansvarig ansvarar därtill för att studenterna får vägledning i frågor som rör:

a) Vilka personuppgifter som är nödvändiga att samla in och behandla för att uppfylla ändamålet med arbetet samt underbygga slutsatserna i detsamma.

b) När inhämtade personuppgifter ska raderas med hänsyn till behovet av att kunna styrka slutsatserna i arbetet.

26 §

Mejl, skriftliga omdömen, anteckningar och annan dokumentation rörande student ska vara adekvat och relevant samt formuleras med respekt för studentens personliga integritet. Sådan information bör inte innehålla beskrivningar eller värderingar av studentens personliga egenskaper och förhållanden, andra förhållanden som ligger nära den privata sfären eller känsliga uppgifter som studentens hälsa.

27 §

Mejl, skriftliga omdömen, anteckningar och annan dokumentation rörande student eller annan som innehåller sådana uppgifter som avses i 26 § andra meningen får endast lagras som krypterade mejl enligt 21 §, i W3D3/Diariet eller på F: och G: samt krypterat flyttbart lagringsmedia. I övrigt gäller reglerna för integritetskänsliga personuppgifter sådan information.

Kommentar till 26-27 §§
Aktuell bestämmelse: Datainspektionens beslut/svar i ärende 986-2009 och 619-2105.

Datainspektionen har vid ett par tillfällen haft anledning att uttala sig om skriftliga omdömen av ämneskunskap m.m. De slutsatser som kan dras av detta har kommit till uttryck i ovan regler.

Reglerna innebär bl.a. att information som innehåller känsliga eller personliga och privata uppgifter om en student, eller andra, inte får föras över eller lagras i Ping Pong.

Kompletterande regler inom forskning

28 §
Med forskning menas vetenskapligt arbete för att inhämta ny kunskap och utvecklingsarbete, med undantag för sådant arbete som endast utförs inom ramen för högskoleutbildning på grundnivå eller avancerad nivå.

29 §
Handledare för doktorand ansvarar för att doktoranden får klar och tydlig information om hur doktoranden ska behandla personuppgifter för forskningsändamål enligt högskolans beslutade regler.

Kommentar
Aktuell bestämmelse: HB-regel

Högskolan ansvarar för doktoranders behandling av personuppgifter inom ramen för sin forskarutbildning. Det innebär att högskolan vid risk för sanktionsavgifter och skadestånd har att tillse att doktorander behandlar personuppgifter enligt högskolans beslutade regler.

Till skillnad från studenter som genomför utbildning på grundnivå eller avancerad nivå bedriver doktorander forskning. För forskning gäller de särskilda reglerna i 30-35 §§ samt de övriga reglerna för anställda i tillämpliga delar. Detta gäller oavsett om doktoranden är anställd eller inte vid högskolan. Det är doktorandens handledares ansvar att se till att doktorandens behandling av personuppgifter för forskningsändamål sker enligt dessa regler, t.ex. genom information, instruktioner och vägledning.

30 §
All behandling av personuppgifter som sker med stöd av allmänt intresse ska vara nödvändig. Om ändamålet med forskningen kan uppnås med anonyma uppgifter, ska forskningen bedrivas med sådana uppgifter.

Kommentar
Aktuell bestämmelse: Artikel 6 dataskyddsförordningen

31 §
Vid forskning som bedrivs tillsammans med externa aktörer, ansvarar den eller de som är ansvarig/a för den forskning inom vilken personuppgifter behandlas för att personuppgiftsansvarig/a är utsedd/a och att detta är dokumenterat.

I det fall det inte finns ett dokumenterat ansvar för forskningen, ansvarar den eller de chef/er med verksamhetsansvar inom vilken forskningen bedrivs för dokumentationen av personuppgiftsansvarig/a enligt första stycket.

Kommentar:
Aktuell bestämmelse: HB-regel

Inom ramen för forskning som utförs tillsammans med externa aktörer är det inte givet vem som är personuppgiftsansvarig. Frågan har stor betydelse. Vid bedömningen av vem som är personuppgiftsansvarig kan det bl.a. beaktas vem som är initiativtagare till

forskningen, varför forskningen utförs, vem som bestämmer över hur behandlingen av personuppgifter ska gå till, avtal m.m.

Den som är personuppgiftsansvarig kan överlåta den faktiska behandlingen av personuppgifter, men aldrig ansvaret för densamma. Det är därför alltid den personuppgiftsansvarige som är ansvarig för att lagar och förordningar följs. Detta ansvar innefattar normalt även andra projektmedlemmars behandling av personuppgifter. Det är därför viktigt att det är klart och tydligt vem eller vilka som är personuppgiftsansvarig/a. Kontakta alltid högskolans dataskyddsfunktion vid tveksamheter om vem som är personuppgiftsansvarig eller vad ansvaret innebär.

32 §

Den eller de som är ansvarig/a för den forskning inom vilken personuppgifter behandlas ansvarar för att ansöka om etikprövning när sådan krävs.

I det fall det inte finns ett dokumenterat ansvar för forskningen, ansvarar den eller de chef/er med verksamhetsansvar inom vilken forskningen bedrivs för att ansöka om etikprövning enligt första stycket.

Kommentar
Aktuell bestämmelse: 3-6 §§ etikprövningslagen

All behandling av känsliga personuppgifter för forskningsändamål kräver en godkänd ansökan om etikprövning. Godkänd ansökan om etikprövning krävs också vid forskning på personuppgifter som rör lagöverträdelser samt i några andra fall, se 3-4 §§ etikprövningslagen. En godkänd ansökan om etikprövning krävs oavsett vart i världen själva behandlingen av personuppgifter sker, så länge som den personuppgiftsansvarige (normalt högskolan) har en koppling till EU/EES.

33 §

Följande gäller vid behandling av personuppgifter för forskning enligt 3 §.

Vid insamling eller registrering av personuppgifter ska information om personuppgiftsbehandlingen lämnas den registrerade på lämpligt sätt i samband med registreringen av personuppgifterna. Högskolans mallar för informationen ska användas.

I det fall personuppgifterna inte har tagits emot från den registrerade behöver information inte lämnas om det skulle visa sig vara omöjligt eller medföra en oproportionell ansträngning, eller det sannolikt skulle göra det omöjligt, eller avsevärt svårare att uppfylla ändamålet med personuppgiftsbehandlingen. Ett ställningstagande att inte lämna information ska vara väl motiverat och dokumenterat.

Kommentar
Aktuell bestämmelse: Artikel 12-22 och 34 dataskyddsförordningen

Personer som är föremål för personuppgiftsbehandling inom ramen för forskning har rätt att få information om personuppgiftsbehandlingen, och motsätta sig behandlingen. Detta gäller oavsett vilken rättslig grund behandlingen vilar på. Det är bara om det är omöjligt, eller det skulle medföra en oproportionerlig ansträngning, eller om ändamålet med behandlingen inte går att uppfylla om man ger forskningspersonen information och möjlighet att motsätta sig behandlingen, som information inte behöver lämnas.

Det är den som avser att behandla personuppgifter som har att bedöma om information om behandlingen inte kan lämnas. Det är viktigt att göra en ordentlig bedömning och kunna motivera den. I det fall tillsynsmyndigheten inte skulle dela bedömningen är behandlingen olaglig. Högskolan kan då bli skadeståndsskyldig mot de vars personuppgifter behandlats felaktigt samt få betala kraftiga sanktionsavgifter till staten.

34 §

Den eller de som är ansvarig/a för den forskning inom vilken personuppgifter behandlas ansvarar för att rutin för hur information som innehåller personuppgifter samlas in, registreras, lagras, delas, arkiveras och raderas, finns dokumenterad och att berörda känner till den.

I det fall det inte finns ett dokumenterat ansvar för forskningen, ansvarar den eller de chef/er med verksamhetsansvar inom vilken forskningen bedrivs för dokumentationen m.m. enligt första stycket.

Kommentar

Aktuell bestämmelse: Artikel 5 (principerna om uppgifts- och lagringsminimering samt principen om integritet och konfidentialitet), 24, 32 och 89 dataskyddsförordningen. 3 och 30 §§ arkivlagen, Riksarkivets föreskrifter i tillämpliga delar samt högskolans informationshanteringsplan

Högskolan är ansvarig för att skyddet av personuppgifter alltid är tillräckligt för de personuppgifter som behandlas. Forskning bedrivs inte sällan inom ramen för projekt, eller liknande former, där flera medarbetare och ofta externa aktörer är inblandade. Detta ställer krav på att det finns tydliga rutiner som ger praktisk vägledning om hur personuppgiftsbehandlingen ska gå till för att den ska kunna ske säkert och korrekt.

Inom forskning kan en stor mängd olika information som innehåller personuppgifter förekomma. Exempelvis grunddata som intervjusvar, patientjournaler, enkäter, statistik, sammanställningar, beräkningar eller ljud och bildupptagningar. Det kan också vara fråga om administrativa handlingar som anslagsansökningar, avtal, projektplaner, dagböcker, mötesprotokoll, minnesanteckningar, olika slags rapporter, ekonomisk redovisning, korrespondens, utkast, koncept, forskningspublikationer eller information på webben, bloggar och i sociala medier. För all denna information ska det således finnas rutiner.

Information som innehåller personuppgifter inom forskning ska lagras, arkiveras och raderas m.m. på samma sätt som övrig information, se särskilt avsnitten ”lagring, arkivering och radering” samt ”mejl och sociala medier”.

35 §
Vid behandling av personuppgifter för forskningsändamål ska personuppgifterna pseudonymiseras eller omfattas av andra lämpliga skyddsåtgärder, under förutsättning att ändamålet med forskningen fortfarande kan uppnås på så sätt.

Kommentar
Aktuell bestämmelse: Artikel 6.1 e) och 89.1 dataskyddsförordningen

Pseudonymisering innebär att personuppgifterna inte kan kopplas till en specifik individ utan att man använder kompletterande information, ”en kodnyckel”. Kodnyckeln bör förvaras tekniskt och organisatoriskt avskild, om möjligt.

Kompletterande regler för systemutveckling

36 §
Utveckling och test av IT-system, applikationer, verktyg, tjänster och dylikt bör så långt det är möjligt utföras på ett sätt som innebär att personuppgifter inte behöver behandlas.

37 §
Personuppgifter som behandlas för utvecklings- eller teständamål får inte lagras längre än nödvändigt. Personuppgifter bör raderas efter utförd behandling.

38 §
Utveckling och test bör ske åtskilt från produktionsmiljön.

Kommentar 36-38 §§
Aktuell bestämmelse: Tillsynsmyndighetens praxis

Kravet på att personuppgifter som behandlas för utvecklings- och teständamål inte får lagras längre än nödvändigt innebär att personuppgifter bör raderas efter att behandlingen ifråga utförts, t.ex. utveckling eller test av en specifik och avgränsad funktion.

Anmälan av personuppgiftsbehandling

39 §
Nya, ändrade eller inaktuella behandlingar av personuppgifter enligt högskolans register över personuppgiftsbehandlingar ska anmälas till, och godkännas av, dataskyddskyddshandläggare av den som avser att utföra sådan behandling.

Kommentar
Aktuell bestämmelse: Artikel 24 dataskyddsförordningen

Högskolan är skyldiga att föra ett register över alla aktuella/pågående behandlingar av personuppgifter på högskolan. Registret har inledningsvis tagits fram utifrån en kartläggning av personuppgiftsbehandlingen vid högskolan vintern 2017/18.

Av registret framgår följande:

1) för vilka ändamål personuppgifter behandlas, t.ex. rekrytera personal, genomföra kurstillfälle eller arrangera evenemang osv.
2) på vilken rättslig grund personuppgifter behandlas, t.ex. samtycke eller allmänt intresse.
3) vilka personuppgifter som behandlas, t.ex. namn, personnummer eller uppgifter om hälsa.
4) vilka personer uppgifter behandlas om, t.ex. anställda eller studenter.
5) vilka som tar emot och behandlar personuppgifter, t.ex. anställda.
6) vilka IT-system personuppgifter behandlas i, t.ex. Ping Pong.
7) vilket IT-system personuppgifter ska arkiveras i, t.ex. Diariet.
8) vid vilken tidpunkt personuppgifter raderas.

De registrerades rättigheter

40 §
En mottagen begäran från en registrerad om att utöva sina rättigheter ska skyndsamt skickas till arkiv och registratur.

41 §
Varje medarbetare ska skyndsamt bistå dataskyddsfunktion med den hjälp som är nödvändig för att hantera och tillgodose de registrerades rättigheter.

Kommentar
Aktuell bestämmelse: Artikel 15-18, 20-22 och 24 dataskyddsförordningen

Alla personer som högskolan behandlar personuppgifter om har ett antal rättigheter. Exempelvis har de rätt att få utdrag över vilka personuppgifter som behandlas och på vilket sätt. De har också rätt att begära att deras uppgifter ändras, kompletteras, raderas eller att behandlingen begränsas eller upphör helt. Flera rättigheter är inte undantagslösa och kräver att högskolan utreder och fattar beslut i frågan. I samband med detta ska vissa tidsfrister och andra krav iakttas. Det är därför viktigt att en begäran från en person som vill utöva sina rättigheter skyndsamt tas om hand för handläggning av densamma. Dessutom är det viktigt att medarbetare skyndsamt bistår med den hjälp som behövs för att högskolan ska kunna tillgodose de registrerades rättigheter. Exempelvis kan systemförvaltare och forskare m.fl. behöva bistå med information om en registrerad.

UPPFÖLJNING

Aktuella bestämmelser: Artikel 24 dataskyddsförordningen.

Högskolan ansvarar för, och ska kunna visa, att all behandling av personuppgifter sker på ett säkert och korrekt sätt i enlighet med dataskyddsförordningen. För att

det ska vara möjligt krävs viss uppföljning av behandlingen av personuppgifter vid högskolan.

Vid användning av högskolans IT-system uppstår behandlingshistorik (”loggar”). Dessa loggar innehåller bl.a. uppgift om användarnamn, tidpunkt, åtgärd, och om åtgärden lyckades eller misslyckades. Loggarna analyseras regelbundet för att upptäcka, utreda, begränsa, rapportera och i övrigt hantera incidenter. I samband med misstänka incidenter kan fler uppgifter behöva hämtas in.

Utöver detta kan slumpmässiga kontroller av enskilda medarbetares behandling av personuppgifter utföras. Syftet med detta är i första hand att upptäcka och åtgärda systemfel genom information och utbildning samt tekniska och organisatoriska åtgärder.

Beslut om slumpmässig kontroll fattas av högskolans dataskyddsombud. Chef för HR, de aktuella medarbetarnas chef/er, huvudskyddsombud samt fackliga organisationer ska konsulteras innan sådant beslut fattas.

Slumpmässig kontroll utförs av högskolans dataskyddsombud med bistånd av IT-avdelningen. Kontrollen ska därvid ske med hänsyn till medarbetares integritet. Eventuella brister dokumenteras, rapporteras och följs upp inom ramen för högskolans systematiska dataskyddsarbete samt på sektionsnivå eller motsvarande.

INDEX