Aluehallintovirasto
Regionförvaltningsverket
Regional State Administrative Agency

EU:s nya dataskyddsförordning

Tammerfors 15.2.2018

Thomas Sundell

Jurist

Regionförvaltningsverkens
svenska enhet för bildningsväsendet

Vad är det fråga om?

- GDPR (General Data Protection Regulation) godkändes 2016 och träder i kraft i maj 2018
- I egenskap av EU-förordning tillämpas den direkt och behöver inte implementeras i nationell lagstiftning
- Behandlingen av personuppgifter har tidigare reglerats via ett EU-direktiv, vilket har kunnat leda till vissa skillnader i lagstiftningen mellan medlemsstaterna

GDPR:s förhållande till nationell lagstiftning

- Till viss del tillåts och förutsätts att medlemsstaterna preciserar GDPR i nationell lagstiftning
- Sedan februari 2016 finns en arbetsgrupp för verkställande av EU:s dataskyddsförordning (TATTI), som gav ett betänkande i juni 2017
- Olika instanser har gett utlåtande om betänkandet, men något förslag till dataskyddslag har ännu inte getts
- Den ursprungliga tanken var att den nuvarande personuppgiftslagen ersätts med dataskyddslagen samtidigt som GDPR träder i kraft

Aluehallintovirasto
Regionförvaltningsverket
Regional State Administrative Agency

Del I

Nuläget: Personuppgiftslagen 523/1999

Tillämpningsområde

- Personuppgiftslagen (PUL) tillämpas på
  - automatisk behandling av personuppgifter
  - manuell behandling av personuppgifter som hör eller är tänkta att höra samman i ett personregister
- Gäller till skillnad från offentlighetslagen inte bara myndigheter
- PUL tillämpas om registeransvariges verksamhetsställe lyder under finländsk jurisdiktion eller en aktör utanför EU har anordningar i Finland (= servrar) som används också för annat än ren förmedling av datatrafik

Undantag från tillämpningsområdet

- PUL tillämpas inte alls på behandling som en fysisk person gör uteslutande för personliga eller därmed jämförbara ”sedvanliga privata syften”
  - Gränsdragningen kan ibland vara svår och borde också beakta hur privatpersoners interaktion på internet ändras med tiden
- På behandling för redaktionella, konstnärliga och litterära syften tillämpas endast delar av PUL
  - Ett sådant syfte bör kunna styrkas

Personuppgifter

- § Personuppgifter är ”alla slags anteckningar som beskriver en fysisk person eller hans egenskaper eller levnadsförhållanden som kan hänföras till honom själv eller till hans familj eller någon som lever i gemensamt hushåll med honom”
- § Förutom uppenbara saker som namn, adresser, födelsetider och liknande är exempelvis foton också personuppgifter

Personregister

- § Ett personregister är ”en datamängd som innehåller personuppgifter och som består av anteckningar som hör samman på grund av sitt användningsändamål, och som helt eller delvis behandlas med automatisk databehandling eller har ordnats som ett kartotek, en förteckning eller på ett annat motsvarande sätt så att information om en bestämd person kan erhållas med lätthet och utan oskäliga kostnader”
- § Formen saknar betydelse – det kan vara allt från ett datasystem till en samling blanketter eller ett häfte

Behandling av personuppgifter

- § Som behandling av personuppgifter räknas ”insamling, registrering, organisering, användning, översändande, utlämnande, lagring, ändring, samkörning, blockering, utplåning och förstöring av personuppgifter samt andra åtgärder som vidtas i fråga om personuppgifterna”
- § Definitionen torde täcka in så gott som allt man kan göra med personuppgifter
- § PUL:s definition verkar dock utgå från en klassisk föreställning om dataregister som inte synligt beaktar internet

Registeransvarig och ansvarspersoner

- § Registeransvarig innebär ”en eller flera personer, sammanslutningar, inrättningar eller stiftelser för vilkas bruk ett personregister inrättas och vilka har rätt att förfoga över registret eller vilka enligt lag ålagts skyldighet att föra register”
- § Definitionen säger inte explicit huruvida det måste vara en fysisk eller juridisk person
- § I speciallagstiftning, t.ex. EoSVL, kan det finnas krav på ansvarspersoner, som INTE är samma sak utan en utnämnd person som fungerar som kontaktperson

Planering och ändamålsbundenhet

- § Behandling av personuppgifter måste hänga samman med den registeransvariges verksamhet
- § Innan man börjar samla in eller ordna uppgifter måste man definiera användningsändamålet och vilka av den registeransvariges funktioner behandlingen tjänar
- § Personuppgifter får endast användas eller i övrigt behandlas i enlighet med användningsändamålet
- § Senare behandling av personuppgifter för historisk forskning eller för vetenskapliga eller statistiska syften anses inte stå i strid med de ursprungliga ändamålen

Relevanskrav och felfrihetskrav

- § Alla uppgifter som behandlas ska behövas med tanke på registrets användningsändamål (relevanskrav)
  - Det är inte ens med samtycke tillåtet att behandla uppgifter som är onödiga
- § Den registeransvarige ska se till att man inte behandlar uppgifter som är oriktiga, ofullständiga eller föråldrade (felfrihetskrav)
  - Bedömningen ska göras med beaktande av användningsändamålet och behandlingens betydelse för den registrerades integritetsskydd

Utlämnande av uppgifter

- Uppgifter ur ett personregister får lämnas ut endast i enlighet med registrets användningsändamål
- På enskilda uppgifter i ett personregister tillämpas offentlighetslagen
- Då en offentlig uppgift som finns i en myndighets personregister begärs som utskrift eller kopia ska man utreda identitet och användningsändamål (OffL 16 § 3 mom) samt hur uppgifterna kommer att skyddas
  - Då uppgifter ges som kopia, utskrift eller i elektronisk form måste mottagaren ha rätt att behandla dem

Grunder för behandling av personuppgifter

§ Enligt PUL 8 § får personuppgifter endast behandlas:

- med entydigt samtycke av den registrerade
- på uppdrag av den registrerade eller för att fullgöra ett avtal där den registrerade är part
- om det i ett enskilt fall är nödvändigt för att trygga den registrerades vitala intressen
- om behandlingen är lagstadgad eller behövs för att fullgöra en skyldighet som någon har påförts i lag eller med stöd av lagen

Grunder för behandling av personuppgifter

§ forts...

- på basis av ett kund- eller tjänstgöringsförhållande, ett medlemskap eller liknande så att den registrerade har en saklig anknytning till den registeransvariges verksamhet (*anknytningskrav*)
- om det är fråga om uppgifter om kunder hos eller arbetstagare vid en koncern eller någon annan ekonomisk sammanslutning och dessa uppgifter behandlas inom nämnda sammanslutning

Grunder för behandling av personuppgifter

§ forts...

- om behandlingen behövs för betalningstjänst, databehandling eller jämförbara uppgifter som utförs på uppdrag av den registeransvarige
- om det är fråga om en allmänt tillgänglig uppgift som beskriver en persons ställning och uppgifter inom ett offentligt samfund eller inom näringslivet och dessa uppgifter behandlas för att trygga rättigheter och intressen hos den registeransvarige eller en sådan tredje man till vilken uppgifterna lämnas ut
- med tillstånd av datasekretessnämnden

Känsliga personuppgifter

§ I PUL 11 § definieras som känsliga uppgifter sådana uppgifter som beskriver eller vilkas syfte är att beskriva:

- ras eller etniskt ursprung
- samhällelig eller politisk uppfattning, religiös övertygelse eller medlemskap i fackförbund
- brottslig gärning eller straff eller annan påföljd för brott
- hälsotillstånd, sjukdom, handikapp eller vårdåtgärder
- sexuell inriktning eller beteende
- behov av socialvård eller tjänster, stödåtgärder och förmåner inom socialvården som någon fått

Undantag gällande känsliga personuppgifter

§ Trots förbudet i 11 § tillåts:

- behandling som den registrerade har samtyckt till (observera dock relevanskravet)
- behandling av uppgifter om samhällelig eller politisk uppfattning, religiös övertygelse eller medlemskap i ett fackförbund som den registrerade själv offentliggjort
- behandling av uppgifter som behövs för att skydda en persons vitala intressen och den inte kan samtycka
- behandling av uppgifter för rättsliga anspråk

Undantag gällande känsliga personuppgifter

§ forts...

- behandling som regleras i lag eller som föranleds av en uppgift som har ålagts den registeransvarige i lag
- behandling för forskning eller statistikföring
- behandling inom föreningar av uppgifter om religiös övertygelse, politisk eller samhällelig uppfattning eller medlemskap i fackförbund, om de gäller medlemmar, om de har samband med föreningarnas syften och de inte lämnas ut

Undantag gällande känsliga personuppgifter

§ forts...

- behandling inom hälsovården av uppgifter om hälsotillstånd och vårdåtgärder eller andra nödvändiga uppgifter
- behandling på en försäkringsanstalt av uppgifter som är nödvändiga för att utreda dess ansvar
- behandling inom socialvården av uppgifter om behov av tjänster, stödåtgärder eller förmåner eller andra nödvändiga uppgifter
- behandling med tillstånd av datasekretessnämnden

Utplåning av känsliga personuppgifter

- § Personuppgifter som klassas som känsliga ska utplånas så snart det inte finns någon grund för behandlingen
- § Grunden för och behovet av behandling ska bedömas minst vart femte år, om inte något annat följer av lag eller ett tillstånd av datasekretessnämnden
  - Exempelvis finns det listor över handlingar inom social- och hälsovården som ska sparas varaktigt eller en längre tid, och de finns antingen i lag eller i förordning som har getts med stöd av lag

Behandling av personbeteckning

- Personbeteckningen är inte sekretessbelagd men behandlingen regleras i PUL: den får behandlas med samtycke eller med stöd av lag, samt
  - för att utföra en i lag angiven uppgift
  - för att uppfylla den registrerades eller registeransvariges rättigheter och skyldigheter
  - för forskning eller statistikföring
- Vissa branscher nämns specifikt
- Ska inte i onödan antecknas i handlingar

Behandling för särskilda ändamål

- Med vissa begränsningar får personuppgifter behandlas för forskning, statistik, myndigheters planerings- och utredningsuppgifter, personmatriklar, släktforskning och direktmarknadsföring också utan en grund enligt PUL 8 §
- Den registrerade kan förbjuda insamling och registrering av personuppgifter för personmatriklar, släktforskning, marknads- och opinionsundersökningar samt direktmarknadsföring (förbudsrätt)

Översändande till stater utanför EU

- Personuppgifter får översändas till stater utanför EU eller EES endast om staten i fråga tryggar en tillräcklig dataskyddsnivå
  - Uppgifternas art, ändamålet, behandlingens tidsmässiga längd, ursprungslandet och målet, branschspecifika regler och skyddsåtgärder ska beaktas
- Kan till exempel gälla olika molntjänster
- Det finns liknande undantag som för annan behandling

Rätt till insyn

- § Var och en har rätt att få veta vilka uppgifter om hen eller barn i hens vårdnad som har registrerats i ett personregister – eller att sådana inte finns
  - Sekretessbestämmelserna är inget hinder
  - Avgift (högst självkostnadspris) får tas endast om det gått mindre än ett år sedan senaste begäran
- § Begäran ska vara egenhändigt undertecknad eller framföras personligen (inte telefon eller e-post)

Rätt till insyn

- § Den registeransvarige ska utan obefogat dröjsmål ge tillfälle att ta del av uppgifterna eller ge dem skriftligen
- § Om den registeransvarige vägrar ge uppgifterna ska man ge ett skriftligt intyg om detta där orsaken anges
  - Om den registeransvarige inte inom tre månader har gett ett skriftligt svar jämställs det med en vägran
- § Den registrerade kan med hjälp av intyget föra saken till dataombudsmannen, som vid vite kan förelägga den registeransvarige att ge insyn i registret
  - Beslutet kan överklagas hos förvaltningsdomstolen

Rätt till insyn

§ Rätt till insyn finns inte om informationen eller uppgifterna
- kan skada statens säkerhet, försvaret eller den allmänna ordningen och säkerheten eller försvåra förebyggande och utredning av brott
- kan medföra allvarlig fara för den registrerades hälsa eller vård eller någon annans rättigheter
- används uteslutande för forskning eller statistik
- används för tillsyns- och kontrolluppgifter och vägran är nödvändig för statens viktiga ekonomiska intressen

Rätt till rättelse av uppgifter

- § Den registeransvarige ska utan obefogat dröjsmål på eget initiativ eller på yrkande av den registrerade rätta, utplåna eller komplettera en personuppgift som med hänsyn till ändamålet med behandlingen är oriktig, onödig, bristfällig eller föråldrad
  - Obekväm är inte samma som oriktig
- § Om man vägrar är processen samma som för insynsrätt
- § Om det inte är omöjligt eller oskäligt besvärligt ska den registeransvarige meddela om rättelsen till sådana som uppgiften har lämnats ut till

Registerbeskrivning

§ Den registeransvarige ska för varje personregister göra en registerbeskrivning, av vilken det framgår
  – registeransvariges och eventuella företrädares namn och kontaktinformation
  – ändamålet med behandlingen
  – en beskrivning av grupperna av registrerade och de uppgifter som hör samman med dessa
  – vart uppgifter i regel lämnas ut och huruvida uppgifter översänds till stater utanför EU eller EES
  – en beskrivning av principerna för skyddet av registret

Information om behandling

- Registerbeskrivningen ska hållas allmänt tillgänglig
  - Webbplats, anslagstavla...
- Vid insamling av personuppgifter ska den registrerade få uppgifter om de saker som står i registerbeskrivningen plus information om hur den registrerade utövar sina rättigheter (upplysningsplikt)
- I praktiken kan man uppfylla upplysningsplikten genom att göra en dataskyddsbeskrivning i stället för en registerbeskrivning och hålla den tillgänglig

Datasäkerhet

- § Den registeransvarige ska genomföra de tekniska och organisatoriska åtgärder som behövs för att skydda personuppgifterna mot obehörig åtkomst och mot förstöring, ändring, utlämnande och översändande som sker av misstag eller i strid med lag
- § Hänsyn ska tas till tillgängliga tekniska möjligheter, kostnader, uppgifternas mängd, art och ålder samt behandlingens betydelse för integritetsskyddet
- § Kraven finns inte specificerade någonstans och ingen myndighet ger grönt ljus – det handlar om riskminimering

Tekniska anslutningar

- En myndighet kan enligt 29 § i offentlighetslagen ge en annan myndighet tillgång till uppgifter genom en teknisk anslutning, det vill säga direkttillgång till ett register
- Teknisk anslutning kräver samtycke av den registrerade, alternativt en uttrycklig bestämmelse i lagen om rätt att lämna ut uppgifter genom teknisk anslutning (GrUL 41 a §, GymnL 33 a §, YrkUtbL 110 §, EoSVL 21 §)
- Innan behandlingen inleds ska den registeransvarige ges utredningar, förbindelser och i övrigt tillräckliga garantier för att uppgifterna skyddas på korrekt sätt

Del II

GDPR: Vad är nytt jämfört med PUL?

Tillämpningsområde

- Det materiella tillämpningsområdet är i grunden lika
  - Verksamhet som inte hör till unionsrätten är utesluten
  - Vissa typer av myndighetsverksamhet är utesluten
  - Ny definition för undantaget för privat behandling: ”[...] som en fysisk person utför som ett led i verksamhet av rent privat natur eller som har samband med hans eller hennes hushåll”
- UKM anser att tillämpningen på utbildning är oklar, eftersom utbildningen inte torde omfattas av unionsrätten
- Det territoriella tillämpningsområdet utökas

Personuppgiftsansvarig och -biträde

- Personuppgiftsansvarig är en ny term för registeransvarig; en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter
  - Flera aktörer kan också vara gemensamt personuppgiftsansvariga (26 art), bara ansvarsfördelningen är fastställd och kommunicerad
- Personuppgiftsbiträde är en aktör som behandlar uppgifter för den personuppgiftsansvariges räkning

Nya definitioner

- Definitionerna av personuppgifter och behandling är mer omfattande och beaktar bättre såväl den digitala världen som användningen av genetiska och biometriska data
- Definitionen av ett register beaktar sk. logiska register, det vill säga register som utgörs av flera funktionellt eller geografiskt separerade delregister med ett gemensamt ändamål

Principerna för dataskydd

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Lagringsminimering
- Korrekthet
- Integritet och konfidentialitet
- Ansvarsskyldighet
- Privacy by design

Grunder för behandling

- § Grunderna för behandling är likartade som de i PUL: samtycke, avtal, rättsliga förpliktelser och skyddande av intressen som är av grundläggande betydelse för den registrerade eller någon annan
- § Dessutom är behandling tillåten för att utföra en uppgift av allmänt intresse eller som ett led i personuppgiftsansvariges myndighetsutövning
- § En skild grund som gäller den personuppgiftsansvariges eller annans berättigade intressen tillämpas inte hos offentliga myndigheter

Grunder för behandling

- Medlemsstaterna får ha mer specifika bestämmelser gällande behandling för att uppfylla rättsliga förpliktelser eller utföra uppgifter av allmänt intresse eller för myndighetsutövning
- Om inte ovannämnda grunder regleras i unionsrätten ska de preciseras i nationell lagstiftning

Särskilda kategorier av personuppgifter

- Det som i PUL kallas känsliga personuppgifter heter i GDPR ”särskilda kategorier av personuppgifter” (9 art)
- Behandling av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning är förbjuden
- Uppgifter om brott och straff får en särställning (10 art)

Särskilda kategorier av personuppgifter

- Undantagen till förbudet regleras i artikel 9.2 och motsvarar i hög grad undantagen i PUL
- Undantaget som gäller lagstadgad behandling är mer strikt formulerad än i PUL och verkar förutsätta att själva behandlingen är lagstadgad, inte bara verksamheten
- UKM har i ett utlåtande till TATTI-gruppen lyft fram många sammanhang där det inom bildningssektorn är nödvändigt att behandla personuppgifter som gäller hälsotillstånd och övertygelse

UKM:s paragrafförslag

Tietosuoja-asetuksen 9 artiklan 1 kohtaa ei sovelleta, korkeakouluja lukuun ottamatta, rekisteröidyn terveyttä tai uskonnollista tai filosofista vakaumusta koskevien tietojen käsittelyyn, joka on tarpeen tietojen käsittelijälle laissa säädetyn opetuksen, koulutuksen, oppilas- ja opiskelijahuollon tai varhaiskasvatuksen järjestämiseksi. Käsiteltäessä tässä tarkoitettuja arkaluonteisia tietoja rekisterinpitäjän tulee rajoittaa tiedon saanti niihin henkilöihin, jotka tarvitsevat tietoa lakisääteisen työtehtävänsä suorittamiseksi.

§ Paragrafen behövs eftersom det generella undantaget för behandling på grund av lagstadgade uppgifter är borta

Skärpta krav på giltiga samtycken

- Om behandlingen grundar sig på samtycke måste samtycket kunna bevisas
- Begäran om samtycke måste läggas fram så att den tydligt kan särskiljas, i en begriplig och lättillgänglig form och med klart och tydligt språk
- Den registrerade kan när som helst återkalla sitt samtycke och man måste informera om möjligheten
  - Ett återkallande är dock inte retroaktivt
- Samtycke i ett avtal till en för avtalet onödig behandling av personuppgifter är inte nödvändigtvis frivilligt

Barn och informationssamhällets tjänster

- Barn under 16 år kan inte själva samtycka till behandling av personuppgifter i fråga om det som kallas ”informationssamhällets tjänster” (i praktiken t.ex. molntjänster och sociala medier), utan för dessa krävs vårdnadshavarnas samtycke
- Medlemsstaterna får dock sänka åldersgränsen ända ner till 13 år, och det har föreslagits både i Sverige och Finland att gränsen ska vara just 13 år
- Personuppgiftsansvariga ska göra rimliga ansträngningar för att kontrollera vårdnadshavarens samtycke

Information om behandlingen

- § Den personuppgiftsansvarige ska ge information om principerna för behandlingen och hur den registrerade utövar sina rättigheter enligt förteckningar i artiklarna 13 (då uppgifter samlas in av den registrerade) och 14 (då uppgifter om den registrerade samlas in annanstans)
- § Informationen ska ges i en koncis, klar och tydlig, begriplig och lättillgänglig form och med ett klart och tydligt språk, särskilt då den riktas till barn
- § Informationen ska vara skriftlig och kan vara i elektronisk form där det är lämpligt

Den registrerades rättigheter

- § Den registrerade har rätt till 1) tillgång, 2) rättelse, 3) radering, 4) begränsning av behandling och 5) dataportabilitet (punkt 5 gäller inte myndigheter)
- § Den personregisteransvarige ska utan dröjsmål men senast inom en månad meddela vilka åtgärder som vidtagits med anledning av en begäran
- § Om inga åtgärder vidtas ska den registrerade meddelas om orsaken och möjligheten att söka ändring
- § Utövandet av rättigheterna ska vara gratis om inte begäran är uppenbart ogrundad eller orimlig

Rätt till tillgång

- § Ny term för rätt till insyn; den registrerade har rätt att få bekräftelse på huruvida personuppgifter om hen behandlas och i så fall få tillgång till personuppgifterna och viss information om behandlingen (åtta punkter i artikel 15.1)
- § Den registrerade ska få en kopia av uppgifterna – för ytterligare kopior som den registrerade begär får man ta ut en rimlig avgift för administrativa kostnader
- § Rätten till en kopia ska inte ”inverka menligt på andras rättigheter och friheter”

Rätt till rättelse

- § Den registrerade har rätt att utan onödigt dröjsmål få felaktiga personuppgifter som rör hen rättade
- § Den registrerade ska med beaktande av ändamålet med behandlingen ha rätt att komplettera ofullständiga personuppgifter bland annat genom att tillhandahålla ett kompletterande utlåtande
- § Motsvarar i princip regleringen i PUL, men verkar inte ställa samma krav på rättelse på eget initiativ

Rätt till radering (”rätten att bli bortglömd”)

- § Den registrerade har rätt att utan onödigt dröjsmål få sina personuppgifter raderade bland annat om
  - de inte längre är nödvändiga för ändamålet
  - behandlingen bygger helt på samtycke och det återtas
  - de har behandlats på olagligt sätt
  - de har samlats in i samband med erbjudande av informationssamhällets tjänster
- § Om personuppgifterna har offentliggjorts ska rimliga åtgärder vidtas för att underrätta andra om begäran

Begränsningar av rätten att bli bortglömd

§ Rätten att bli bortglömd gäller inte till den del behandlingen är nödvändig bland annat

- för att utöva rätten till yttrande- och informationsfrihet
- för att uppfylla en rättslig förpliktelse enligt unionsrätten eller nationell rätt
- för arkivändamål av allmänt intresse, forskning eller statistik
- för att kunna fastställa, göra gällande eller försvara rättsliga anspråk

Rätt till begränsning av behandling

§ Den registrerade har rätt att kräva att behandlingen begränsas om

- den registrerade bestrider uppgifternas korrekthet, medan personuppgiftsansvarige utreder saken
- behandlingen är olaglig men den registrerade inte vill att uppgifterna raderas
- uppgifterna inte annars längre behövs men den registrerade behöver dem för rättsskyddsändamål
- den registrerade har invänt mot grunden om det handlar om allmänt intresse eller myndighetsutövning

Dataskydd

- Den personuppgiftsansvarige och eventuella personuppgiftsbiträden ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken
  - Bygger på en riskbedömning som bör uppdateras
  - Den senaste utvecklingen, kostnader, behandlingens art, omfattning, sammanhang och ändamål samt riskernas allvar och sannolikhetsgrad ska beaktas
- Godkända uppförandekoder (40 art) och certifiering (42 art) kan användas för att påvisa en viss säkerhetsnivå

Dataskydd

- Principen om inbyggt dataskydd och dataskydd som standard innebär att man identifierar och beaktar behoven och kraven redan i planeringsskedet, innan behandlingen inleds
- I utformningen av den tänkta behandlingen bör man tillämpa GDPR:s dataskyddsprinciper, t.ex. att minimera mängden uppgifter, behandlingens omfattning, lagringstiden och tillgängligheten, att pseudonymisera där det låter sig göras osv.

Ansvarsfördelning vid entreprenad

- Den personuppgiftsansvarige har helhetsansvaret för att behandlingen sker i enlighet med GDPR
- Om behandlingen har lagts på entreprenad så att det finns ett personuppgiftsbiträde måste det finnas ett skriftligt avtal som reglerar behandlingen
- Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan skriftligt tillstånd av den personuppgiftsansvarige

Register över behandling

- § Organisationer som sysselsätter mer än 250 anställda, som behandlar särskilda kategorier av personuppgifter eller vars behandling sannolikt medför risker för registrerades rättigheter och friheter måste ha ett register över den behandling av personuppgifter som utförs
- § Ordet ”register” är lite missvisande – det är inte fråga om en logg utan om något som påminner om en registerbeskrivning enligt PUL och som är en del av den dokumentation som krävs för tillsyn
- § Kraven finns listade i artikel 30

Skyldighet att anmäla incidenter

- § Personuppgiftsincidenter måste utan dröjsmål och om möjligt inom 72 timmar anmälas till tillsynsmyndigheten om det inte är osannolikt att incidenten får några följder
  - Vid förseningar måste förseningen motiveras
  - Innehållet i anmälan listas i artikel 33
- § Om incidenten sannolikt leder till en hög risk för fysiska personers intressen ska också registrerade informeras, i första hand personligen men annars via allmänheten

Konsekvensbedömning

- Om en typ av behandling sannolikt leder till en hög risk ska den personuppgiftsansvarige före behandlingen göra en konsekvensbedömning enligt artikel 35
  - Gäller särskilt vid automatisk behandling (inkl. profilering) eller omfattande behandling av särskilda kategorier av personuppgifter
- Om konsekvensbedömningen visar på hög risk krävs samråd med tillsynsmyndigheten
- Tillsynsmyndigheten ska ha en lista över sådana typer av behandling som kräver konsekvensbedömning

Dataskyddsombud

- Myndigheter och sådana aktörer som i stor omfattning behandlar särskilda kategorier av personuppgifter ska utnämna ett dataskyddsombud, vars uppgift är att handleda personalen, övervaka att man följer GDPR och fungera som kontaktlänk både till de registrerade och till tillsynsmyndigheten
- Kan ingå i personalen eller jobba på basis av tjänsteavtal
- En koncern får ha ett enda dataskyddsombud om det på varje etableringsort är lätt att nå denna person, och myndigheter får med hänsyn till organisationsstruktur och storlek ha gemensamma dataskyddsombud

Ersättningsskyldighet

- § Den som har lidit materiell eller immateriell skada till följd av brott mot GDPR har rätt till ersättning
- § I nuvarande PUL tillämpas strikt ansvar – ersättning utgår oberoende av om någon har gjort något fel – men i GDPR gäller vållande med omvänd bevisbörda: den personuppgiftsansvariga ska visa att den inte på något sätt är ansvarig för den händelse som orsakade skadan
- § Personuppgiftsansvariga och personuppgiftsbiträden som har medverkat i samma behandling är solidariskt ansvariga

Administrativa sanktionsavgifter

- I stället för eller utöver de korrigerande befogenheter tillsynsmyndigheten har kan den påföra en administrativ avgift på upp till 20 miljoner euro eller 4 % av den globala årsomsättningen
  - I bedömningen av avgiftens storlek beaktas bl.a. överträdelsens karaktär, svårighet och varaktighet, uppsåt, lindrande åtgärder, tidigare överträdelser, ekonomisk vinning och hur saken kom fram
- Varje medlemsstat får avgöra i nationell lagstiftning huruvida sanktionsavgifterna tillämpas på myndigheter

Läs mera

- GDPR-förordningen: http://eur-lex.europa.eu/legal-content/SV/TXT/?uri=CELEX%3A32016R0679
- Dataombudsmannens material om GDPR: http://tietosuoja.fi/sv/index/euntietosuojauudistus.html
- TATTI-betänkandet: http://julkaisut.valtioneuvosto.fi/handle/10024/80098
- UKM:s utlåtande (nr 21 under ”Asiakirjat”): http://oikeusministerio.fi/hanke?tunnus=OM006:00/2016