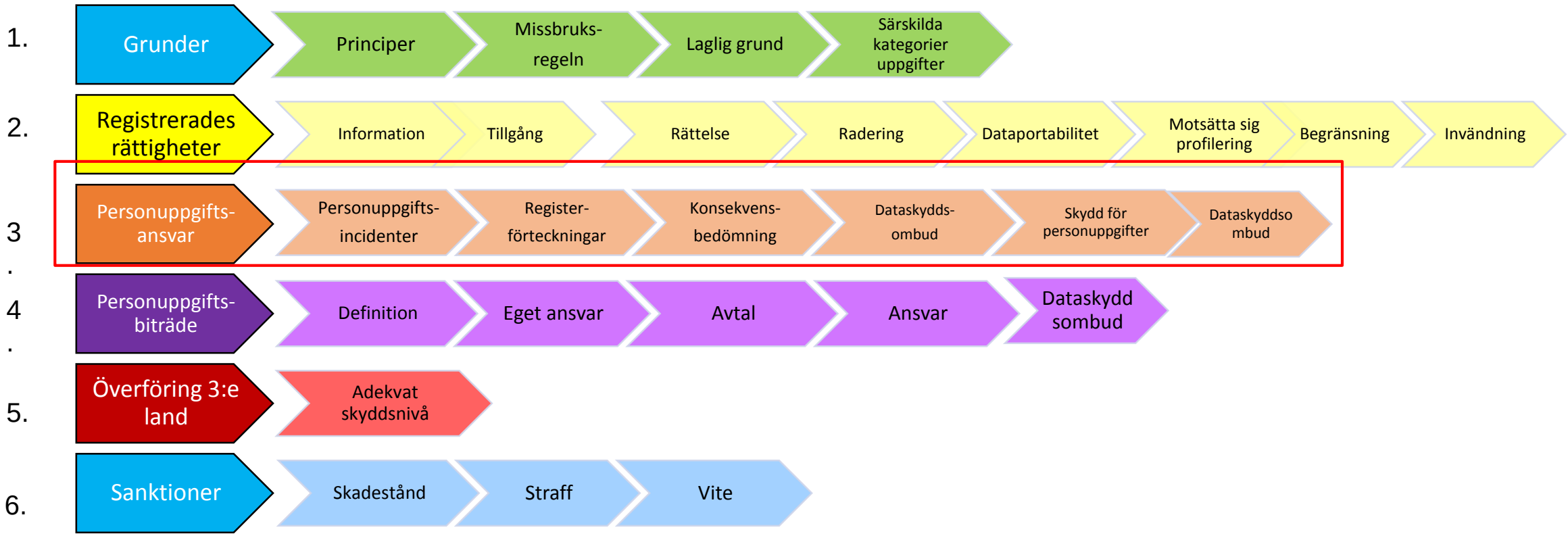
Personuppgiftsansvaret och GDPR

2017-11-02

MANOLIS
NYMARK
CONSULTING

Personuppgiftsansvarigs skyldigheter enligt DSF



Agenda - Personuppgiftsansvaret

1. Vem är personuppgiftsansvarig, och när?

2. Laglighetsprövningen m.m.

3. Skyldigheter enligt DSF

Dataskyddsförordningen (DFS/GDPR)

- Träder i kraft den 25 maj 2018
- Det är en EU-förordning – gäller som lag i Sverige och andra EU/EES-länder
- Gäller alla – myndigheter, företag, föreningar och privatpersoner
- Innehåller 99 artiklar och 173 ”skäl” samt många subartiklar
- Kraftiga vitessanktioner vid brott mot regelverket
- Flera nya skyldigheter och rättigheter

Dataskyddsförordningen (DFS/GDPR)

- PUL och nuvarande dataskyddsdirektivet upphör 25 maj 2018!
- Nuvarande registerförfattningar (ca 200 stycken) ses över
- Nationell reglering krävs eller får förekomma inom vissa områden
- Den personuppgiftsansvarig ansvarar inte bara för att de grundläggande principerna följs utan också ska kunna visa att de efterlevs, s.k. ansvarsskyldighet.
- Ny europeisk dataskyddsstyrelse

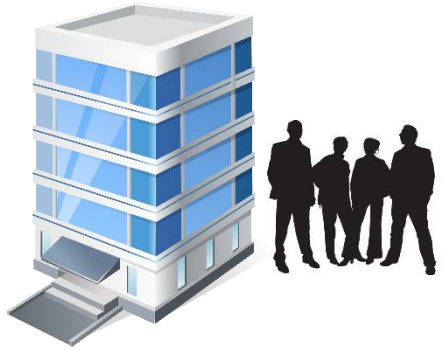
Personuppgiftsansvarig (art 4)

- Definition:

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; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt

1. Vem är personuppgiftsansvarig…och när?

Den som **faktiskt** bestämmer över personuppgifts-behandlingen



2Secure

- I rubricerat rättsfall angående **bakgrundskontroller** hävdade bolaget att det inte var personuppgiftsansvarig eftersom det var deras kunder som beställde bakgrundskontroller. De var **personuppgiftsbiträde.**

- Datainspektionen: Även om uppdragsgivarna tillhandahåller grundinformation och har möjlighet att skräddarsy omfattningen av personuppgiftsbehandlingen, innebär det sagda att bolaget har **en sådan självständig ställning** och kan bestämma ändamålen med och medlen för behandlingen av personuppgifter på ett sådant sätt att bolaget är att betrakta som personuppgiftsansvarigt för tjänsten screening.

- Kammarrätten i Stockholm (2014-01-09) ansåg att eftersom det är bolaget som tillhandahåller tjänsten och därmed ytterst bestämmer över ändamålen och medlen för behandlingen av personuppgifterna, är bolaget att anse som personuppgiftsansvarig

Vem är personuppgiftsansvarig…och när?

Den som **faktiskt** bestämmer över personuppgifts-behandlingen

Även när man inte faktiskt bestämmer över **alla delar** av behandlingen

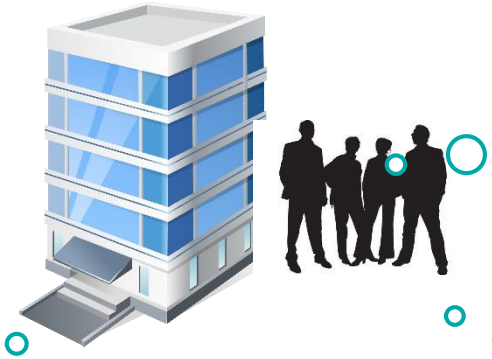
”Utsträckt” personuppgiftsansvar

- HFD 2012 ref. 21: Försäkringskassan har vid tillhandahållande av elektroniska självbetjäningstjänster ansetts personuppgiftsansvarig för den behandling som sker **innan uppgifterna blir tillgängliga för kassan**.

Vem är personuppgiftsansvarig…och när?

Den som **faktiskt** bestämmer över personuppgifts-behandlingen

Även när man inte faktiskt bestämmer över **alla delar** av behandlingen



Ibland **reglerat i lag** VEM som är personuppgiftsan-svarig

Oftast en organisation

Ska behandla ”**personuppgifter**”

Automatiserat eller **strukturerad samling** av personuppgifter, som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier

Rättsfall

Fråga om behandling av personuppgifter har prövats i AD 2013 nr 19 angående behandling av uppgifter om alkoholtester

- Datum, klockslag, registreringsnummer och testresultat skulle sammantaget kunna vara personuppgifter eftersom registreringsnumret möjliggör identifiering av chauffören till exempel med hjälp av DHL:s tjänstgöringslistor.

- Det har emellertid i målet framkommit att uppgifterna från en alkoholtestning endast innehåller datum, klockslag och resultat samt endast antecknas på ett papper för att därefter sättas in i en pärm.

- Det har inte framkommit att pappret sätts in i någon annan ordning än kronologisk ordning. Behandlingen är alltså inte automatiserad.

- Oavsett om uppgifterna är personuppgifter eller inte enligt personuppgiftslagens mening, ingår dessa inte i, eller är avsedda att ingå i, en strukturerad samling av personuppgifter, som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Det innebär enligt Arbetsdomstolens mening att personuppgiftslagen, i enlighet med vad som anges i 5 § den lagen, inte är tillämplig i detta fall.

Vem är personuppgiftsansvarig…och när?

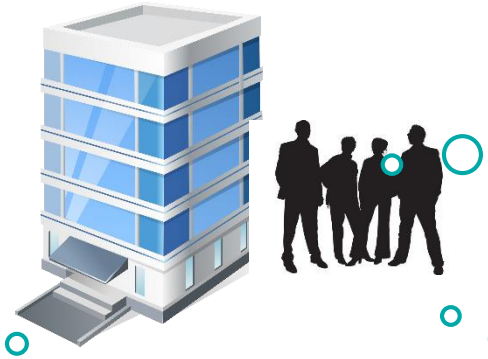
Den som **faktiskt** bestämmer över personuppgifts-behandlingen

Även när man inte faktiskt bestämmer över **alla delar** av behandlingen

Inget personuppgiftsansvar

-offentlighetsprincipen

- ”Eget utrymme” (TF 2:10)????



Ibland **reglerat i lag** VEM som är personuppgiftsan-svarig

DSF har utvidgat **geografiskt tillämpningsområde** – omfattar aktörer utanför EU/EES som tillhandahåller tjänster till EU-medborgare

Automatiserat eller **strukturerad samling** av personuppgifter, som är tillgängliga för sökning eller sammanställning enligt särskilda kriterier

Ska behandla ”**personuppgifter**”

Oftast en organisation

2. Laglighetsprövning – ”Integritetstrappan”

REGISTRERADES RÄTTIGHETER – 8 STYCKEN

ÖVERFÖRING TILL 3:E LAND

PERSONNUMMER, UPPGIFTER OM BROTT

SÄRSKILDA KATEGORIER AV UPPGIFTER – LAGLIG GRUND?

TILLÅTEN BEHANDLING – LAGLIG GRUND? REGISTERFÖRFATTNING?

IAKTTA GRUNDLÄGGANDE DATASKYDDSPRINCIPER – 6 STYCKEN

Sex dataskyddsprinciper (art. 5)

- Personuppgiftsansvariga ska ansvara för och kunna visa att följande principer efterlevs (*ansvarsskyldighet*).

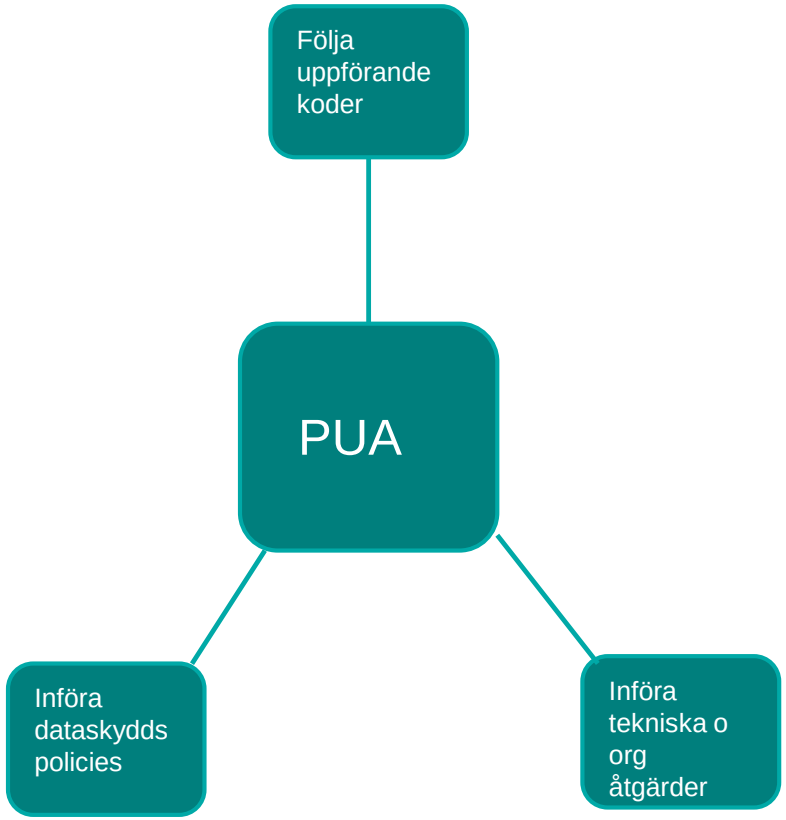
1. Laglighet, korrekthet, öppenhet
2. Ändamålsbegränsning
3. Uppgiftsminimering
4. Korrekthet
5. Lagringsminimering
6. Integritet och konfidentialitet

Åtta rättigheter för registrerade!

1	• Rätt till information, art 13-14
2	• Rätt till tillgång, art. 15
3	• Rätt till rättelse, art 16
4	• Rätt till radering (bortglömd), art. 17
5	• Rätt till begränsad behandling, art 18
6	• Rätt till dataportabilitet, art. 20
7	• Rätt att göra invändning, art. 21
8	• Rätt att slippa automat. beslut, inbegripet profilering, art. 22

3. Den personuppgiftsansvariges ansvar (art 24)

- Bedöma riskerna med behandlingar av personuppgifter för enskildas fri- och rättigheter.
- Lämpliga tekniska och organisatoriska åtgärder ska genomföras för att försäkra och kunna visa att behandlingen följer DSF
- Åtgärderna ska ses över och uppdateras vid behov
- Åtgärderna ska komma till uttryck i lämpliga strategier för dataskydd (dataskyddspolicy, eng. Data Protection Policies).
- Godkända uppförandekoder eller godkända certifieringsmekanismer uppmuntras för att kunna visa ansvarsskyldighet!
- Skadestånd och höga sanktionsavgifter ska inpränta ansvarsskyldigheten!



Rapportera personuppgiftsincidenter (art. 33)

Vägledning finns!

- **Personuppgiftsincident definition**, art. 4: ”En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats”

- **Incidenter som Inte ska rapporteras** - osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter

- Personuppgiftsansvarig ska rapportera till Datainspektionen utan onödigt dröjsmål, dock inte senare än 72 timmar efter vetskap om händelsen.

- (Personuppgiftsbiträde ska informera den personuppgiftsansvarige utan dröjsmål – ingen 72-timmarsfrist).

Personuppgiftsincidenter (art. 33)

- Anmälan till tillsynsmyndigheten (Datainspektionen) ska åtminstone:
  - beskriva personuppgiftsincidentens art
  - beskriva kategorier och ungefärligt antal registrerade,
  - kategorier av och ungefärligt antal uppgiftsposter
  - förmedla kontaktuppgifter för dataskyddsombudet
  - beskriva de sannolika konsekvenserna
  - beskriva föreslagna eller vidtagna åtgärder

Personuppgiftsincidenter (art. 33)

- Registrerade ska som huvudregel informeras om det föreligger hög risk för deras rättigheter och friheter t.ex:
  - att den enskilde förlorar kontrollen över sina uppgifter
  - att hans eller hennes rättigheterna inskränks
  - att den registrerade utsätts för diskriminering, identitetsstöld eller bedrägeri
  - att den registrerade råkar ut för finansiell förlust, skadlig ryktesspridning, brott mot sekretess eller tystnadsplikt

- Information behövs inte om t.ex.
  - Den personuppgiftsansvarige har genomfört lämpliga tekniska och organisatoriska skyddsåtgärder och dessa åtgärder tillämpats på de personuppgifter som påverkades av personuppgiftsincidenten, i synnerhet sådana som ska göra uppgifterna oläsbara för alla personer som inte är behöriga att få tillgång till personuppgifterna, såsom kryptering.
  - ISO 27001 och ITIL möter kraven på ”lämpliga tekniska och organisatoriska skyddsåtgärder”

- Personuppgiftsincidenten ska dokumenteras så att Datainspektionen kan kontrollera efterlevnad (art. 33.5)

Registerförteckning (art. 30)

- **Personuppgiftsansvarig** och eventuella företrädare ska föra ett register över behandlingar av personuppgifter

- Följande uppgifter ska dokumenteras

a) namn och kontaktuppgifter för personuppgiftsansvarig, ev. företrädare och ev. dataskyddsombud
b) ändamålen med behandlingen
c) kategorier av registrerade och kategorier av personuppgifter
d) kategorier av mottagare
e) ev. överföring till tredjeland samt dokumentation av skyddsåtgärder
f) tidsfrist för radering (om möjligt)
g) tekniska och organisatoriska säkerhetsåtgärder

Registerförteckning (art. 30) - undantag

- Företag som sysselsätter färre än 250 personer behöver inte upprätta registerförteckning om inte:

  - Behandlingen sannolikt kommer att medföra en risk för registrerades rättigheter och friheter,
  - Behandlingen inte är tillfällig…eller
  - Behandlingen omfattar särskilda kategorier av uppgifter eller fällande domar i brottmål eller överträdelser.

Konsekvensbedömning avseende dataskydd (art. 35)

Vägledning finns!

- Om en typ av behandling sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den **personuppgiftsansvarige** före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifte. Särskilt vid:
  - Systematisk och omfattande bedömning av personer
  - Behandling i stor omfattning av särskilda kategorier av uppgifter, som avses i artikel 9.1, eller av personuppgifter som rör fällande domar i brottmål och överträdelser som avses i artikel 10.
  - Systematiska övervakning av allmän plats i stor omfattning (kamera)

- Datainspektionen ska offentliggöra en förteckning över det slags behandlingsverksamheter som omfattas av kravet på en konsekvensbedömning avseende dataskydd (ännu ej publicerad)

- Dataskyddsombudet ska rådfrågas

Konsekvensbedömning avseende dataskydd (art. 35)

- Bedömningen ska bl.a. innehålla:
  - beskrivning av och ändamålet med behandlingen
  - utvärdering av risk för registrerads rättigheter och friheter
  - åtgärder som planeras för att hantera riskerna

- Om möjligt inhämta synpunkter från de registrerade eller deras företrädare (jfr patientsäkerhetslagen, involvera anhöriga i patientsäkerhetsarbete)

- Förhandssamråd med Datainspektionen om bedömningen visar hög risk mot enskildas fri- och rättigheter. (**Datainspektionen har äskat en lagstadgad tystnadsplikt hos regeringen för förhandssamråd)**

- Många syften: transparens, trovärdighet, dokumentation, säkert, laglig, ökad medvetenhet i organisationen, användas vid upphandling m.m.!!! Publicera? Sekretess?

Dataskyddsombud (art. 37-39)

Vägledning finns!

- Personuppgiftsansvarig och personuppgiftbiträde måste ha ett Dataskyddsombud om:

Landsting och kommuner

  - Myndighet alt. offentligt organ, ej domstolar.
  - Kärnverksamheten är behandling som regelbunden övervakning i stor omfattning
  - Kärnverksamheten är behandling av känsliga uppgifter i stor omfattning (= vårdgivare)

- Om det inte är uppenbart att ett Dataskyddsombud INTE behövs, bör den personuppgiftsansvarige göra en analys av detta.

- Om en Dataskyddsombud utses på frivillig basis (något krav enligt GDPR föreligger inte), gäller samma krav som om det hade varit tvingande.

Dataskyddsombud (art. 37-39)

- Man får ha ett Dataskyddsombud för en koncern, flera företag eller flera nämnder om:
  - Dataskyddsombudet är tillgänglig från alla delar av verksamheten (jfr verksamhetschef i sjukvården – tillgänglig för patienter och personal)
  - Tydligt kan kommunicera med Dataskyddsombud i det språk som tillsynsmyndigheten tillämpar
  - Lämpligt utifrån organisationens omfattning och komplexitet
- Dataskyddsombud kan utgöras av ett team
- Dataskyddsombud kan vara både intern och kontrakterad extern
- Kontaktuppgifter till Dataskyddsombudet ska offentliggöras och meddelas Datainspektionen.

Dataskyddsombud (art. 37-39)

- Är bunden av sekretess eller konfidentialitet vid genomförande av uppdraget.
- Ska rapportera direkt till styrelse eller ledning
- Det är lämpligt att upprätta riktlinjer för Dataskyddsombudets ansvar och uppgifter. Specificera rollen noga!

Krav sammanfattning:

- Självständighet
- Får inte motta instruktioner om arbetets utförande
- Får ha ”tillikauppgifter”, men inte sådana som skapar intressekonflikt
- Egen budget
- Yrkesmässiga kvalifikationer
- Expertkunnande om lagstiftning

Säkerhet för personuppgifter (art. 32)

- 1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt
  - a) pseudonymisering och kryptering av personuppgifter,
  - b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,
  - c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,
  - d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

ISO/IEC 27001 Ledningssystem för informationssäkerhet

Kontinuitetsplanering

Penetration stester

ISO 31000 Riskhantering

- 2.Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
- 3.Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.
- 4.Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbiträdets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

Krav på Inbyggt dataskydd (art. 25)

- Vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.
  - Pseudonymisering och kryptering
  - Konfidentialitet, integritet, tillgänglighet och motståndskraft hos systemen och tjänster
  - Återställning vid incident
  - Löpande testa och utvärdera effektiviteten

- Vid bedömning av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför:
  - oavsiktlig eller olaglig förstöring,
  - förlust eller ändring
  - obehörigt röjande av eller obehörig åtkomst

Krav på Inbyggt dataskydd (art. 25)

- Datainspektionens broschyr Inbyggd integritet (2012):
  - ”Detta kan också uttryckas som att den personuppgiftsansvarige ska låta integritetsfrågor påverka ett it-systems hela livscykel – från förstudie och kravställning via design och utveckling till användning och avveckling.”

Krav på Dataskydd som standard (art. 25)

- Genomföra lämpliga tekniska och organisatoriska åtgärder för att endast de personuppgifter behandlas som är nödvändiga för varje specifikt ändamål med avseende på:
  - antal insamlade uppgifter
  - behandlingens omfattning
  - tiden för lagring
  - uppgifternas tillgänglighet
  - att de inte görs tillgängliga för obegränsat antal enskilda

- Ska genomsyra alla beslut om behandling

Personuppgiftsbiträdesavtal (art. 28.3)

- Personuppgiftsansvarig ska teckna ett skriftligt avtal med personuppgiftsbiträde, och i det ska särskilt anges:
  - föremålet för behandlingen,
  - behandlingens varaktighet,
  - art och ändamål,
  - typen av personuppgifter
  - och kategorier av registrerade,
  - personuppgiftsansvariges skyldigheter och rättigheter anges

- Personuppgiftsbiträdet måste ställa tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder för att uppfylla DSF och skydda den registrerades rättigheter.

- Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgiftsansvarige (art. 28.2) + krav på personuppgiftsbiträdet att informera personuppgiftsansvarig om nya underbiträden – kan invända.

SLUT!