FOYEN

FOYEN

- Vad är Personuppgifter och vad innebär PuL?
- Molnet – när kan det bli det ett problem?
- Vad ska man tänka på vid användning av molntjänster?
- Windows 10 – vad innebär det ur integritetssynpunkt?
- Lärosätenas ansvar
- Specifika funktioner i Windows 10
- E-post, sökmotorer, digital tentamen
- Ny lagstiftning

PERSONUPPGIFTER OCH BEHANDLING

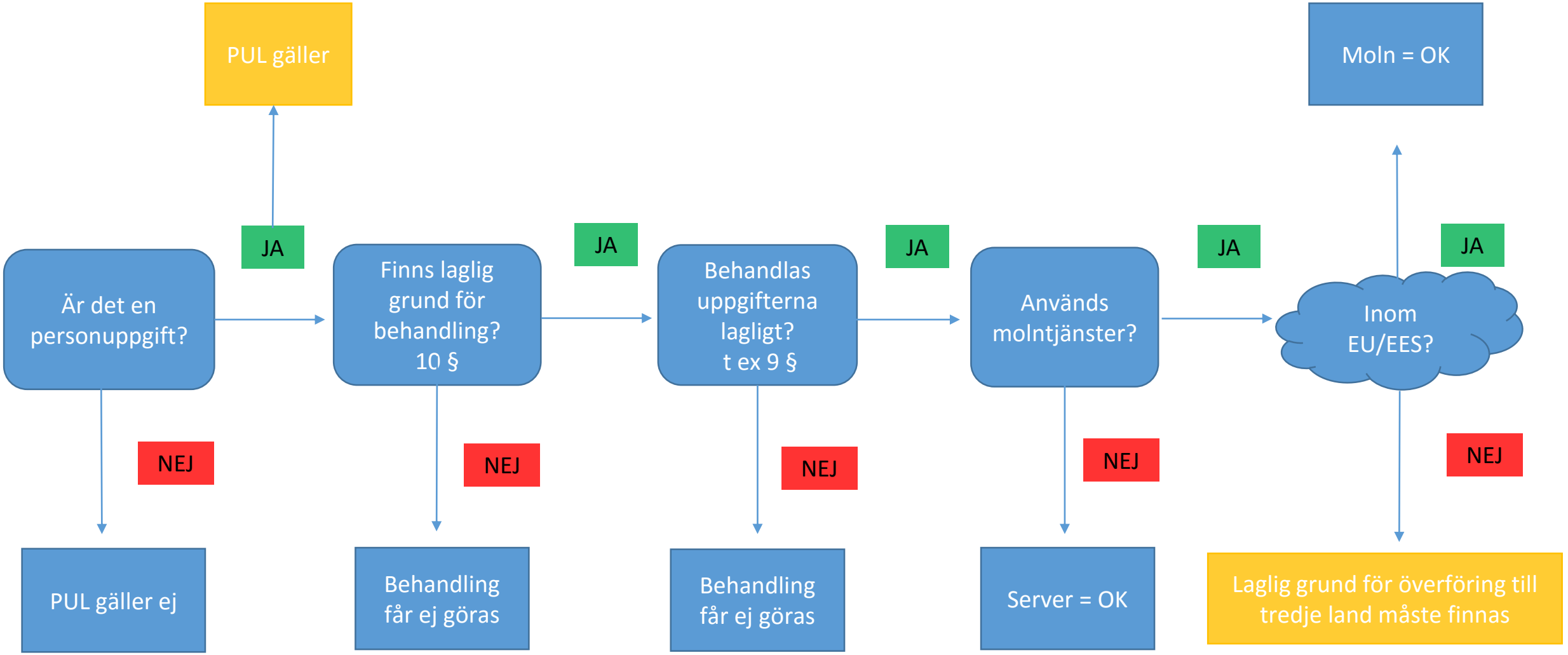
- ”Alla” uppgifter som indirekt eller direkt kan identifiera en fysisk person
  - Namn
  - Telefonnummer
  - E-postadress
  - Adress
  - Personnummer
  - IP-adress….

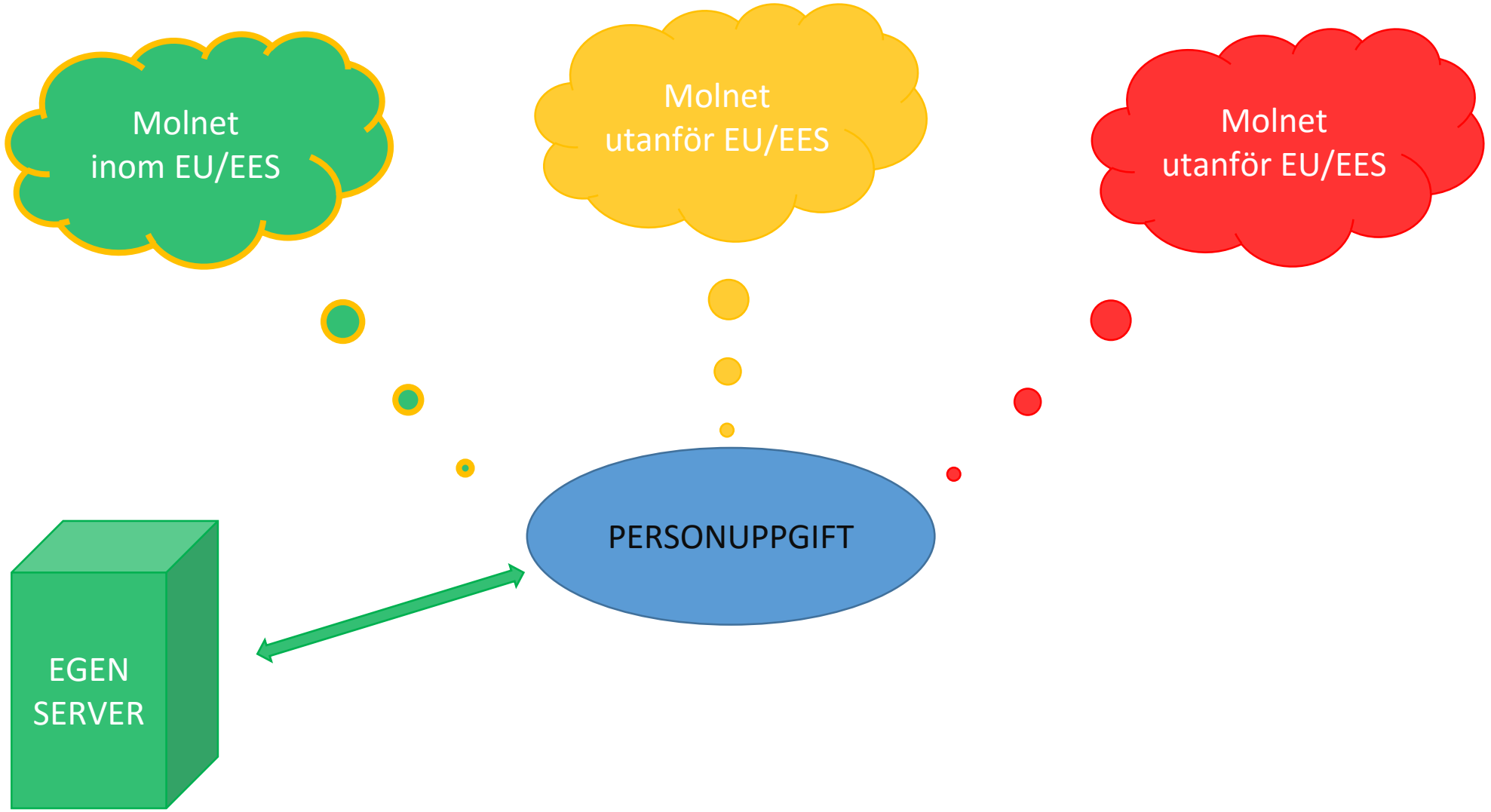
〓 Personuppgift (PU)

- ”Allt” man gör med personuppgifterna
  - Insamling
  - Registrering
  - Lagring
  - Utlämnande…

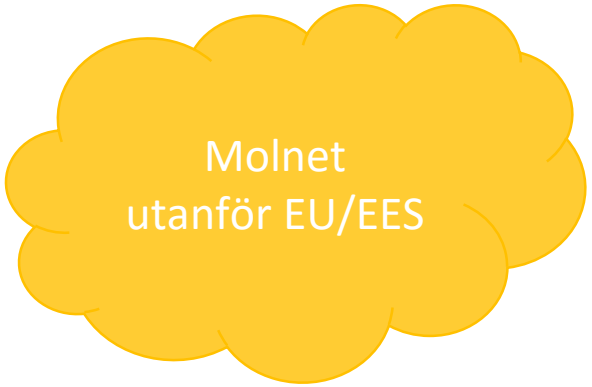
〓 Behandling

FOYEN

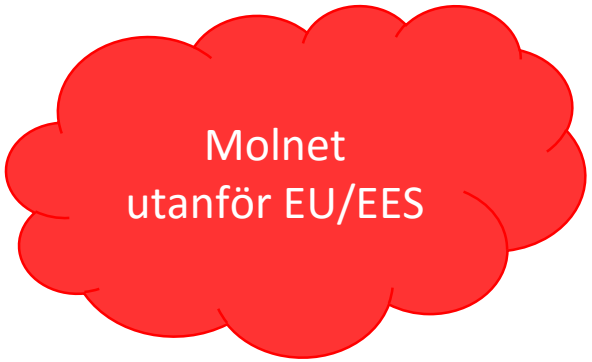

PUL gäller
Moln = OK
JA
JA
JA
JA
JA
Är det en personuppgift?
Finns laglig grund för behandling? 10 §
Behandlas uppgifterna lagligt? t ex 9 §
Används molntjänster?
Inom EU/EES?
NEJ
NEJ
NEJ
NEJ
NEJ
PUL gäller ej
Behandling får ej göras
Behandling får ej göras
Server = OK
Laglig grund för överföring till tredje land måste finnas


Molnet
inom EU/EES
Molnet
utanför EU/EES
Molnet
utanför EU/EES
PERSONUPPGIFT
EGEN
SERVER

FOYEN



1. Om det finns adekvat skyddsnivå enligt t ex EU-kommissionen
2. Om samtycke finns
3. 34§ PUL
4. Om det finns garantier genom att organisation anslutit sig till Standardavtalsklausulerna eller om det finns acceptabla BCR (Binding Corporate Rules)



Om inga av förutsättningarna finns – förbjudet!

ADEKVAT SKYDDSNIVÅ

FOYEN

1. Adekvat skyddsnivå

(EU/EES)

Andorra

Argentina

Bailiwick of Guernsey

Isle of Man

Färöarna

Israel

Jersey

Nya Zeeland

Schweiz

Uruguay

Kanada (om privat sektor och viss lag är tillämplig)

ADEKVAT SKYDDSNIVÅ, FORTS.

Molnet utanför EU/EES

FOYEN

Ny dom från EU-domstolen (”Facebookdomen")

- EU-kommissionen har tidigare beslutat att om en organisation ansluter sig till principerna om Safe Harbour uppfylls kraven på ”adekvat skyddsnivå”
- Facebook-domen 6 oktober 2015 innebär att detta beslut har ogiltigförklarats
- Artikel 29-gruppen har 20/10-15 uttalat att ”överföringar till USA som sker med stöd av EU-kommissionens beslut om Safe Harbour är olagliga”
- ”Överföringar […] till länder vars myndigheter har befogenhet att få åtkomst till information i en utsträckning som går längre än vad som är nödvändigt i ett demokratiskt samhälle kommer inte att anses som en säker destination”.
- Ny Safe Harbour-lösning diskuteras!

FOYEN

2. Samtycke

- Uttryckligt och informerat – den registrerade ska veta vad man samtycker till, dvs ”behandling av uppgifterna sker i molnet i land utanför EU/EES”.

- Frivilligt – alternativ måste finnas (arbetstagare anses ej kunna samtycka!)

- Kan ej samlas in i efterhand

FOYEN

34 § PUL

Om behandlingen är nödvändig för att

- ett avtal ska kunna fullgöras med den registrerade
- rättsliga anspråk skall kunna hanteras (tvist)
- vitala intressen för den registrerade skall kunna skyddas (t ex akuta medicinska skäl)
- samt till en stat som anslutit sig till Europarådets konvention om skydd för enskilda vid databehandling (Marocco, Mauritius och Senegal)

ÖVRIGT

FOYEN

- Standardavtalsklausulerna binder avtalsparten till ”adekvat skyddsnivå”
  (kan läggas in i ett avtal eller användas separat)

- BCR: Lista på företag med godkända BCR finns på
  http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/bcr_cooperation/index_en.htm

- Microsoft - Azure, Office 365, Microsoft Dynamics CRM and Windows Intune?
  - Inte helt godkänt av Artikel 29-gruppen, men Microsoft hävdar detta…

VARFÖR ÄR USA ETT PROBLEM I DETTA SAMMANHANG?

- NSA samlar in stora mängder uppgifter
- Andra amerikanska myndigheter anser sig ha rätt att få ut information från amerikanska bolag, oavsett var servern faktiskt befinner sig (FBI, åklagarmyndigheten i New York). Mål pågår.

- Idag håller inte en amerikansk tjänst, även om servern står i EU, med säkerhet, en ”adekvat skyddsnivå” enligt EU.

- Datainspektionen svarar inte generellt på om villkoren för en molntjänst duger
- Man kan begära samråd med DI om specifik situation

- Ersättning för Safe Harbour diskuteras – lösning behövs!

SÅ KONKRET SOM MÖJLIGT…

- Förutsättning: Lärosätet behandlar personuppgifter på laglig grund och på lagligt sätt

Kan molntjänster användas?

✓Ja, om Molnet är inom EU/EES och under EU/EES-kontroll (och det ej är känsliga uppgifter)

✓Ja, om avtalet med Molntjänsteleverantören garanterar adekvat skyddsnivå

✓Ger Microsoft en adekvat skyddsnivå?

RÅDET IDAG ÄR:

- Om det kan finnas känsliga uppgifter – skicka inte/lagra inte i Molnet (hög risk=olämpligt enl. DI)

- Ej känsliga uppgifter – använd Molnet om det är lagligt, dvs. om uppgifter får föras över till tredje land. (PUBA ska upprättas med Molnleverantör, standardklausuler kan tecknas).

- Anpassa säkerhetsnivån (anpassa Windows 10 t ex)
- Sätt upp interna regler hur vissa typer av uppgifter får behandlas.

- Kontrollera avtalet med Microsoft för de tjänster som används
- Laglighet eller inte beror på tjänsten och personuppgifternas art – generellt svar kan ej ges!

ATT TÄNKA PÅ VID ANVÄNDNING AV MOLNET

FOYEN

1. Ta ställning till om behandlingen är laglig

- Granska avtalet med molntjänstleverantören
- Finns risk för att personuppgifter kan komma att behandlas för andra ändamål än de ursprungliga?
- Kan uppgifterna komma att lämnas över till tredjeland?
- Finns stöd i PUL för tredjelandsöverföring?
- Vilka säkerhetsåtgärder behöver vidtas för att skydda personuppgifter?
- Finns ett PUBA?
- Finns annan relevant lagstiftning, t ex sekretesslagstiftning?

ATT TÄNKA PÅ VID ANVÄNDNING AV MOLNET

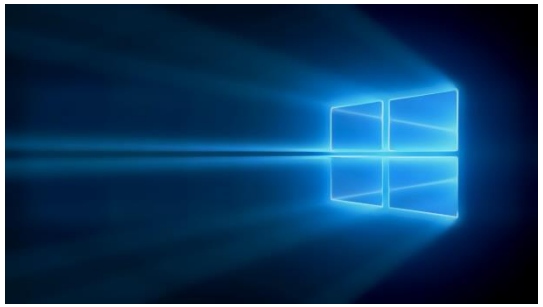
2. Risk – och sårbarhetsanalys

- Antal registrerade
- Mängden uppgifter → Nivå på säkerheten
- Känsligheten i uppgifterna

- Finns checklistor att använda; t ex ENISA Cloud Computing , Information Assurance Framework
- Kontroll av biträdena ska göras - följer man PUBA?

FOYEN

WINDOWS 10 – VAD SAMLAS IN?



- Namn och kontaktuppgifter
- Autentiseringsuppgifter (koder, röst, biometrisk data)
- Demografiska data (ålder, kön, land och språk)
- Intressen och favoriter (vid appanvändning, web-läsare etc.)
- Betalningsdata (kreditkortsnummer, säkerhetskoder)
- Användningsdata (såväl avseende funktioner som används som uppgifter om enheten – prestandarelaterat)
- Kontakter och relationer.
- Positioneringsinformation (kan vara exakt, t ex från GPS, wifi-hotspots)
- Innehåll (t ex i e-post för att kunna leverera)
- Med mera – beroende på vilka tjänster som används

FOYEN

FUNKTIONER I WINDOWS 10

- Windows Hello – biometrisk information (fingeravtryck/iris/ansikte)
  - Ska aktiveras av användaren
- Microsoft Edge (lagring av webbhistorik)
  - Hubben ska aktiveras av användaren
- Office (lagring i OneDrive=Molnet)
  - Ingen aktivering
- Cortana (insamling av stor mängd uppgifter i telefon/PC)
  - Kräver f n särskild aktivering (finns ännu ej för Sverige)

MICROSOFT WINDOWS 10 - VEM ANSVARAR?

- Personuppgiftsansvarig är Microsoft, som bestämmer ändamålen med insamlingen av uppgifter i sina tjänster
- Har anställda något val – finns alternativ till Windows?
- Varje verksamhet behöver arbetsverktyg – alternativen är begränsade. Intresseavvägning mellan arbetsgivarens intresse och de anställdas intresse av skyddad integritet.
- Möjliggöra för den enskilde att begränsa insamling från Microsoft
  (lås ej den typen av funktioner)

LÄROSÄTENAS ANSVAR DÅ?

- För personuppgifterna som de bestämmer ändamålen med (betyg, resultat, etc…)
- Lärosätena bestämmer säkerhetsnivån!
  - Överväg vilka funktioner som ska ”tas bort” i Windows, dvs. anpassa default till så hög säkerhetsnivå som möjligt
    - Koppla bort Cortana?
    - Inloggning lokalt istället för med Microsoft-konto
    - Ta bort koppling till kalender och e-postkonton?

LÄROSÄTENAS ANSVAR, FORTS.

- Om funktioner behövs – kontrollera laglighet
- Om funktioner inte kan tas bort, eller om användaren själva har möjlighet att ändra – reglera internt

  - Policy för e-posthantering
  - Policy för surf
  - Policy för lagring
  - Policy för kamera/mikrofon och positionering…

  - Tydliggör för användare vad som gäller, och vad följden blir om man inte följer detta.
  - Viktigt förklara varför – PUL och Windows-insamling är delvis inkompatibla

FOYEN

PÅVERKA SÄKERHETSNIVÅN!

- Autentisering
- Behörighetsstyrning
- Behörighetskontroll
- Loggning (främst när det är fråga om känsliga uppgifter)
- Kommunikationssäkerhet
- Rutiner för säkerhetskopiering
- Utplåning
- Skydd mot obehörig åtkomst och
- Skadlig programvara

E-POST

- I sig ingen personuppgift
- Kan dock innehålla personuppgifter (tentaresultat t ex)

- Policy ska upprättas (lättfattlig och lättillgänglig)
  - Vad får man skicka? (”Okänsliga” personuppgifter med sedvanligt skydd)
  - Vad måste krypteras? (Känsliga personuppgifter)
  - Vad får inte skickas? (”Känsligare” uppgifter)

- Kan man lita på kryptering? – Njae - Microsoft kan komma att tvingas lämna ifrån sig nyckeln…

BING, GOOGLE ELLER ANNAN SÖKMOTOR

- Innehåller algoritmer som lagrar information och styr träffar
- Svårt hindra användning av sedvanliga sökmotorer, behövs i arbetet
- Mindre känslig information, sökmotorn ansvarig för insamlingen
- Användarens mönster registreras – inte de personuppgifter som Lärosätena ansvarar för

DIGITAL TENTAMEN OCH INLOGGNING

- Tentamen ligger i Molnet (ej personuppgifter i sig)
- Inloggning sker med personuppgifter
- Ansvarig för inloggningen är Lärosätena
    - Personnummer regleras särskilt i PUL
    - Sådan får behandlas med samtycke eller när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller av något annat beaktansvärt skäl

DIGITAL TENTAMEN, FORTS.

- Finns möjlighet till annan legitimering som en innebär behandling av personuppgift (e-leg t ex)?
- Min bedömning är att skäl för behandling normalt sett finns
  - Information om behandlingen ska lämnas vid inloggningen
    - Vem är personuppgiftsansvarig?
    - Ändamålen med behandlingen
    - Ev. övrig information
  - Säkerhet och laglighet
    - Anpassa efter karaktären på PU
    - Om inloggning i Molnet gäller samma sak som för andra PU!

HUR BLIR MAN 100 % SÄKER PÅ ATT GÖRA RÄTT?

- Lagra alla personuppgifter i egen server eller server inom EU/EES
- Avvakta ny EU-Amerikansk lösning…

- Titta på vilka personuppgifter det är och hur de faktiskt behandlas
- Undersök hur leverantörens avtal ser ut
- Fundera på vilken säkerhetsnivå som är lämplig med hänsyn till tekniska möjligheter, känsligheten i uppgifterna, risker och ekonomiska förutsättningar

- Om tveksamt - överväg samråd med Datainspektionen

DATASKYDDSFÖRORDNINGEN 2018 (?)

FOYEN

Ny EU-lagstiftning

- Principerna mycket lika dagens PuL
- Dock mer formalia (dokument ska tas fram och revideras)
- Privacy by Design – inbyggt integritetsskydd

- Hårdare tag mot integritetsbrott;
  - Fängelse
  - Skadestånd
  - Böter (upp till det högsta av 100 000 000 € eller 5% av årsomsättningen)

KONTAKTUPPGIFTER

Advokat Sara Malmgren

Tel: 08-506 184 28

sara.malmgren@foyen.se

www.foyen.se