IT-forum för administrativa chefer

2021-10-30

Stockholms universitet

Presentationen kommer att spelas in

Genomsnittsbetyg för föregående IT-forum för administrativa chefer

4,2 av 5

Stockholms universitet

Syftet med IT-forum för administrativa chefer

1. Öka administrativa chefers kännedom om pågående universitetsgemensamma IT-utvecklingsprojekt
2. Öka administrativa chefers kännedom om hur styrningen av universitetsgemensam IT-utveckling fungerar, inklusive vilka påverkansmöjligheter som finns
3. Stärka administrativa chefer i sitt ansvar kopplat till IT
4. Utgöra tillfälle för IT-avdelningen att samla in åsikter, önskemål och frågor kring universitetsgemensam IT

Stockholms universitet

Agenda

- Introduktion
- Säker informations- och personuppgiftshantering
- Utvecklingsfokus just nu
- Informationspunkter
  - Avgiftshöjning IT-access
- Diskussion

Stockholms universitet

Informationssäkerhet och dataskydd (GDPR)

Björn Gustavsson, Dataskyddsombud

Stockholms universitet

Agenda

1. Samverkan mellan informationssäkerhet och dataskydd
2. Snabbt om regelverken
3. Praktiska saker i ert arbete
4. Avslutande frågor

Informationssäkerhet

- Handlar om att skydda information
- Konfidentialitet, riktighet och tillgänglighet (KRT), ibland också spårbarhet (KRTS)
- Processer, regler, stöd och kunskap.

Konfidentialitet

- Kan delas upp i interna och externa krav.
- Exempel på interna krav: Affärsförhandlingar, konkurrens (uppdragsforskning, -utbildning) och forskningsprojekt och ideer.
- Exempel på externa krav: Sekretess, MSB, Dataskyddsförordningen.

Riktighet

- Uppgift som används ska vara ”rätta” och ”riktiga”
- Externt krav: MSB, Dataskyddsförordningen

Tillgänglighet

- Uppgifterna ska vara tillgängliga när dom behövs.
- Allmänna handlingar, loggar, kontaktlistor m.m.

Spårbarhet

- Det ska gå att spåra hur och när uppgifter har skapats, ändrats och tagits bort.
- Samt av VEM.
- Även loggar som tillgodoser spårbarhet kan ha (KRTS-krav på sig)

Dataskyddsförordningen

- Tillämpbart på alla personuppgifter SU behandlar.
- Personuppgifter är uppgifter om en identifierad eller identifierbar individ. (levande)
- Dataskyddsförordningen ska tillämpas i all hantering av personuppgifter (inkl. inhämtande, lagring och radering)

Principer som kompletteras av detaljer

- Principer
  - Lagligt, korrekt och öppet
  - Insamlade för visst ändamål och sedan inte användas för oförenliga ändamål
  - Adekvata, relevanta och inte för omfattande
  - Korrekta och om nödvändigt, uppdaterade.
  - Lagras så kort tid som möjligt (kom ihåg arkivering)
  - Behandlas på sådant sätt att säkerheten för personuppgifterna är lämplig

SU SKA KUNNA VISA ATT ALLA DESSA PRINCIPER EFTERLEVS!

Registrerades rättigheter

- Rätt att få del av vilka personuppgifter som behandlas om sig
- Rätt att få felaktiga uppgifter rättade
- Rätt att få uppgifter raderade (kom ihåg arkivering)
- Rätt att få behandlingen begränsad (under den tid övriga rättigheter prövas)
- Rätt att göra invändning

VID BEGÄRAN OM RADERING/RÄTTELSE/BEGRÄNSNING MÅSTE SU INFORMERA ALLA MOTTAGARE AV PERSONUPPGIFTEN OM DETTA.

“Detaljer” i urval

- När vi använder en leverantör för att behandlas personuppgifter åt oss ska det finnas ett personuppgiftsbiträdesavtal som omfattar behandlingen.

  Ett vanligt misstag är att bara underteckna en “mall”. Avtalet ska dock innehålla bl a vilka kategorier av personuppgifter som ska behandlas, ändamålen för detta, de säkerhetsåtgärder som bedöms lämpliga för den aktuella behandlingen samt vad som ska hända med uppgifterna när avtalet avslutas. Detta är olika för olika avtalsparter.

“Detaljer” i urval

- Registerförteckning

Stockholms universitet är skyldigt att ha ett aktuellt register över alla personuppgiftsbehandlingar som sker vid myndigheten. Detta ska hållas uppdaterat både avseende vilka behandlingar som sker och detaljerna om dessa.

”Detaljer” i urval

- Överföring till mottagare i land utanför EU/EES

Som huvudregel gäller ett förbud att skicka personuppgifter till en mottagare utanför EU/EES. Undantag gäller för länder som av EU-kommissionen bedömt ha en adekvat skyddsnivå.

Behöver SU trots detta skicka personuppgifter till en mottagare i “tredje land” behöver det finns att avtal ”standardiserade dataskyddsbestämmelser” mellan SU och mottagaren. SU behöver därtill göra en bedömning att rättsordningen i mottagarlandet för att avgöra om lagarna tillsammans med avtalet innebär en skyddsnivå för uppgifterna som är “essentially equivalent”

Incidenter

- Det sker incidenter vid SU I stort sett varje dag!
- Dataskyddsförordningen och MSBs föreskrifter ställer olika krav på incidenter.
- Dataskyddsförordningen: Incident är något som innebär oavsiktlig eller olagligt röjande, ändring, förlust eller förstöring av personuppgifter.

Incidenter fort.

- MSB: IT-incidenter som inneburit påverkan på KRT hos information med behov av utökat skydd, om ett system som använder denna information brustit i funktionalitet, påverkan på myndighetens förmåga att utföra sitt uppdrag och annan allvarlig påverkan på säkerheten.

- Dataskyddsförordningen kräver även klassning av incidenten: hög, normal, och låg. Olika rapporteringskrav gäller då.

- TIDSFRISTER!!! MSB inom SEX (6) timmar. GDPR inom 72 timmar.

Styr- och stöddokument

- su.se/gdpr
- Riktlinjer för informationssäkerhet
- Personuppgiftspolicy
- Säkerhetspolicy

Stockholms universitet

Praktiska saker

- molntjänster
  - Kräver PUB-avtal och påverkas nästan alltid av reglerna om överföring utanför EU/EES
- Vet vad ni ansvarar för
  - Den information ni ansvara för måste ni också tillförsäkra att den lever upp till kraven i regelverken och bevakar dessa.
- Interna och externa krav på er information
  - Genomföra informationsklassning. Oklassad information ska alltid behandlas som om den kräver högsta skyddsnivå.

Praktiska saker

- Hålla koll på era ändamål. Varför ni behandlar personuppgifter, om vem och vilka uppgifter.
  - Detta ska kommuniceras till de registrerade.

- Löpande uppdatera registerförteckningen
  - Den ska alltid vara aktuell

- Arkivera, arkivera, arkivera och GALLRA
  - Genom att skilja bort information från er dagliga verksamhet blir arbetet enklare. Genom att förstöra information som får gallras minskar arbetsbördan.

Praktiska saker

- Gör så lite som möjligt själva
  - Kraven på information kommer bara öka, inte minska. Ta hjälp, hitta samarbeten och dela på ansvaret så mycket det bara går!

- Glöm inte uppgifter om anställda
  - Anställdas personuppgifter ska behandlas enliga samma regelverk.

- Slutligen: MAILA INGET KÄNSLIGT!

Tack för mig

Frågor?

bjorn.gustavsson@su.se

Stockholms universitet

Agenda

- Introduktion
- Säker informations- och personuppgiftshantering
- Utvecklingsfokus just nu
- Informationspunkter
  - Avgiftshöjning IT-access
- Diskussion

Stockholms universitet

Utvecklingsfokus just nu

- Flertalet utvecklingsinitiativ som går ut på att uppgradera och modernisera det universitetsgemensamma systemstödet pågår just nu
- Merparten av initiativen har startats för att befintliga systemstöd är gamla, kostar mycket att upprätthålla, följer inte lagen till fullo eller utgör en verksamhetsrisk
- Gemensamma mål för samtliga initiativ är att
  - Skapa förutsättningar för ökad digitalisering och automatisering
  - Minska risk för driftstörningar och informationsförlust

- Universitetet tar alltså nödvändiga steg mot ökad digitalisering men behöver ha ett starkare fokus och strävan mot nyttorna som kommer med ökad digitalisering

Fokus i pågående verksamhetsnära utvecklingsarbete med IT-inslag

Pågående förstudier/analyser	Genomförda förstudier/analyser 2021	Pågående förändringsinsatser	Genomförda förändringsinsatser 2021
Byte av CMS	Systemstöd för administration av lärarutbildningen	Byte av examinationssystem	Lansering av Kursvärdering
Uppgradera serviceportalen/ ärendehantering	Förbättrat stöd till institutioner i studieadministrativa frågor	Byte av system för utbildningsplanering	Lansering av elektroniska labböcker (ELN)
Nytt telefoniplattform	Införande av e-arkiv	Uppgradera beslutsstödsplattform	Lansering av ”Lagring av forskningsdata”
MS 365	Uppgradera beslutsstödsplattform	Avveckling av Mondo	Lansering av DISP
		Avveckling av Fastreg	Lansering av ny externwebb

Vad vill ni höra mer av?

Stockholms universitet

[1] Inkluderar inte förändringsinsatser som initierats utanför portföljplaneringen (DIM och Ekonomiprojektet)

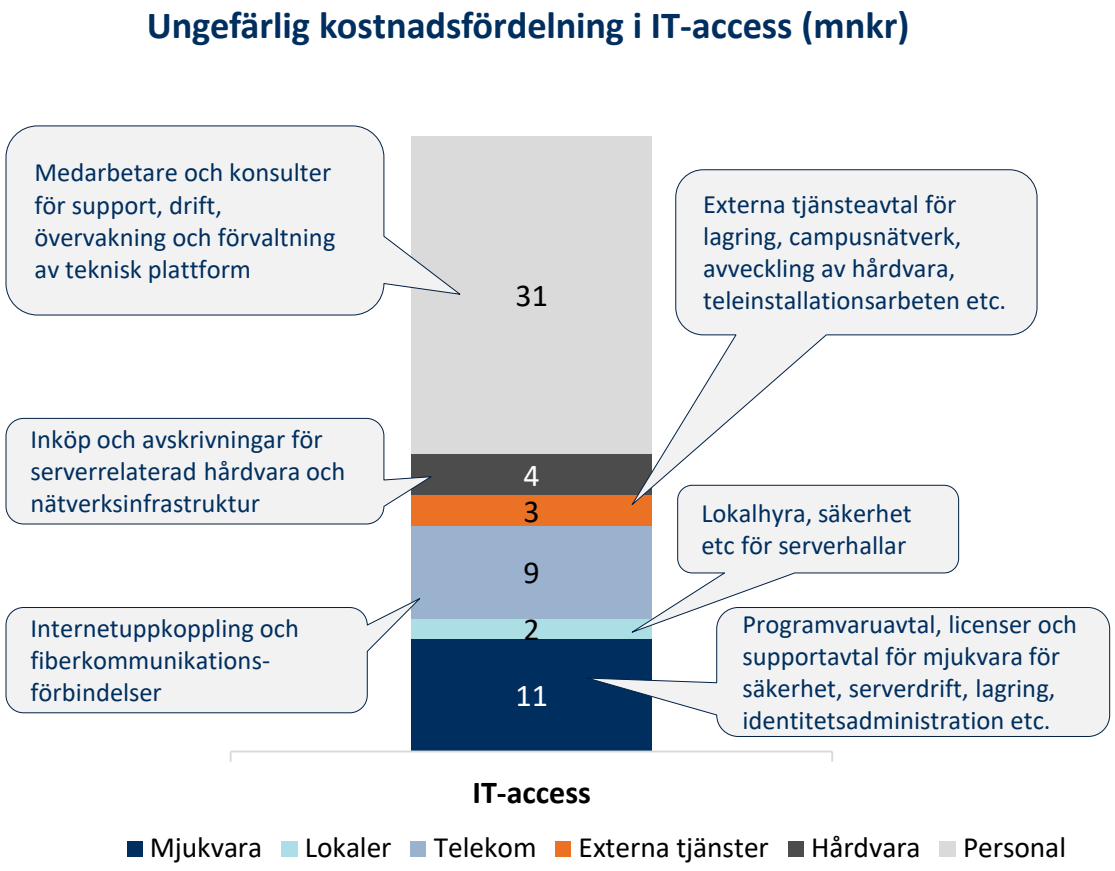
Agenda

- Introduktion
- Säker informations- och personuppgiftshantering
- Utvecklingsfokus just nu
- Informationspunkter
  - Avgiftshöjning IT-access
- Diskussion

Stockholms universitet

Avgiftshöjning IT-access 2022

- 2022 höjs avgift för IT-access (motsvarande 23%)
- Syfte med höjning är att säkerställa kostnadstäckning för ingående tjänster med rörlig kostnadsmassa, säkerhetsrelaterade teknikuppgraderingar och nya uppdrag kring Albano
- Beräkningsgrund för IT-access är antal användare – dvs. institutioner med många studenter, anställda eller anknutna bär större andel av den totala kostnaden
- Det finns idéer om att anpassa beräkningsgrunderna för tjänsten, t.ex. att anknutna ska bära större andel av totala kostnaden



Stockholms universitet

Agenda

- Introduktion
- Säker informations- och personuppgiftshantering
- Utvecklingsfokus just nu
- Informationspunkter
  - Avgiftshöjning IT-access
- Diskussion

Stockholms universitet