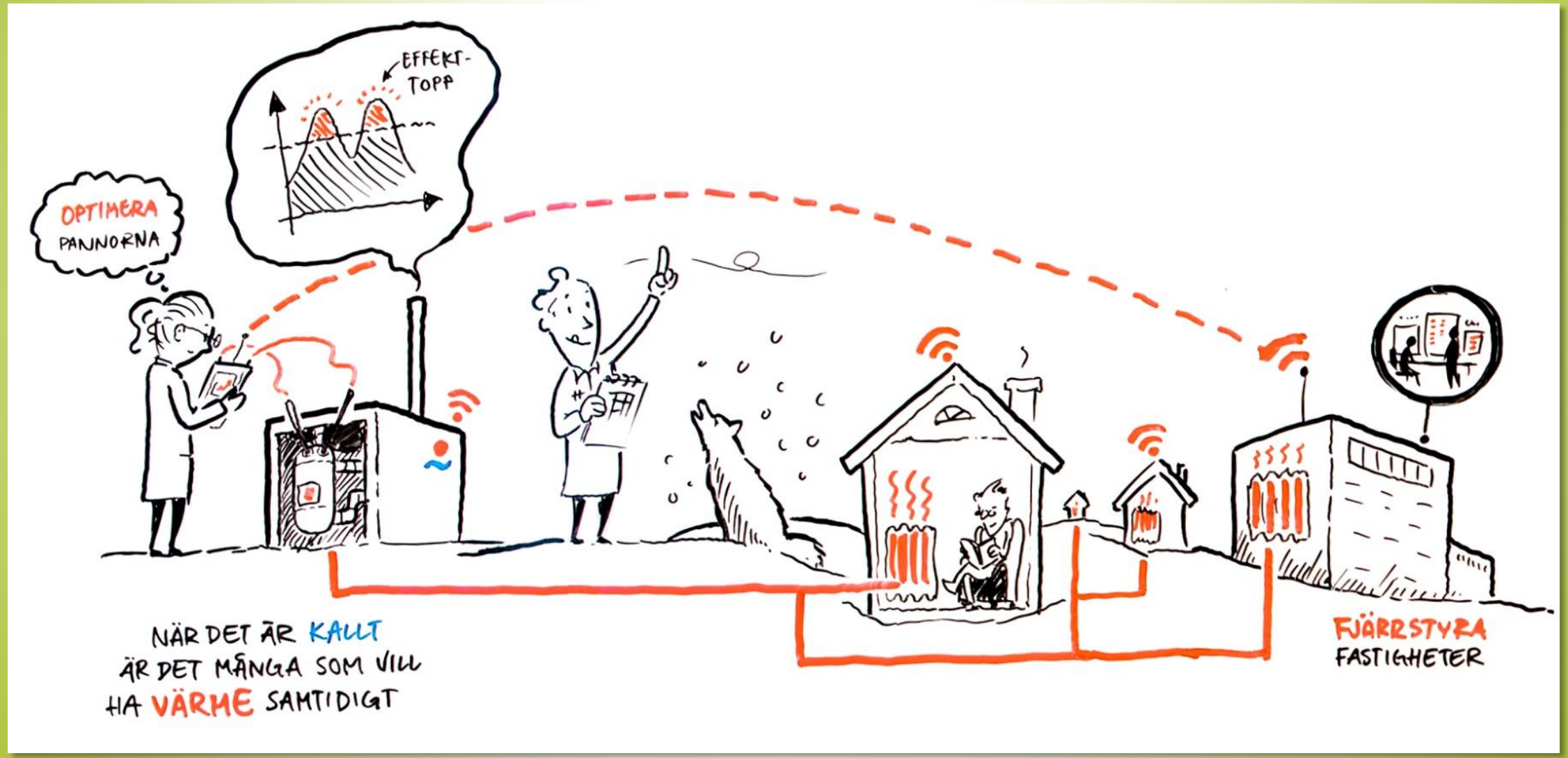
IIOTSP FORUM, DECEMBER 8, 2016

IIoTSP – PUL och EU dataskyddsförordningen

Varför blev PUL intressant i vårt projekt?



Vad är PUL?

Personuppgiftslagen innehåller regler som ska skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter.

Begreppet "behandlas" är brett, det omfattar insamling, registrering, lagring, bearbetning, spridning, utplåning, med mera.

Personuppgiftslagen (PuL) trädde i kraft 1998 och bygger på gemensamma regler som har beslutats inom EU, det så kallade dataskyddsdirektivet.

Vad är en personuppgift?

All slags information som direkt eller indirekt kan hänföras till en fysisk person.

Inte bara personnummer utan även t.ex. Regnummer på bil, IP-nummer, mac-adress, anställningsnr, kreditkortnr räknas som personuppgifter om de kan kopplas till fysiska personer

Även bilder (foton) och ljudupptagningar på individer som behandlas i dator kan vara personuppgifter.

Vad skulle kunna omfattas av PUL i Industrin?

Mätare kopplat till förbrukning
Transporter
Taggar inpassering
Kameror fast installation/fordon
Jämföra olika skiftteam
Materialföljning
Underhåll av maskiner

Förenklar Molnlagring att Lägga Pussel?

Vad säger PUL i mer Detaljer?

Så fort man inte behöver uppgifterna så ska man gallra dem (Bryts av många företag)

Laglig grund för behandling är ex samtycke
obs: anställda kan i princip inte lämna samtycke

Grunden för behandling är att den är Frivillig, specifik och informerad

Andra lagliga grunder: fullgörande av avtal, fullgöra legal skyldighet, utföra uppgift i allmänintresse, den ansvariges legitima intressen (många guidelines på DI för intresse avvägningen)

Vad säger PUL i mer Detaljer?

Informationskrav slarvas det med redan idag. Den registrerade ska få info om Hur länge info sparas, rätten att radera, rätten att bli ”glömd”, rätten till dataportabilitet, rätten till att återta samtycke, rätten till att klaga hos tillståndsmyndigheten

Vilka tekniska/organisatoriska lösningar som krävs av lagen beror på känsligheten på data, vad som är rimligt kostnadsmässigt, vad som är möjligt

Personuppgiftsbiträden kräver personuppgiftsbiträdesavtal

Vad säger PUL i mer detaljer

Kryptering och anonymisering kan göra att risken inte bedöms som hög vid överträdelser och därmed behöver man kanske inte kontakta de som är registrerade

Vite-nivåer kommer att bedömas utifrån tekniska/organisatoriska lösningar som företagen har implementerat

Risk och sårbarhetsanalys ska utföras t.ex. vid storskalig behandling av känsliga personuppgifter

Risk o Sårbarhetsanalys

Risk och sårbarhetsanalys ska utföras t.ex. vid storskalig behandling av känsliga personuppgifter

Innehåller:

- Systematisk beskrivning av behandling inklusive dess ändamål
- Bedömning av nödvändighet och proportionalitet
- Risk för fri- och rättigheter
- Åtgärder för riskhantering

Rekommendation: Gör analysen för att veta vilka tekniska och organisatoriska lösningar som bör implementeras

Vad gör Microsoft Azure för att följa PUL?

Enligt Datainspektionens uppställda krav erbjuder Microsoft ett personuppgiftsbiträdesavtal, Safe Harbor-certifiering, EUs standardskontraktsklausuler och transparens vad gäller datacenter och underleverantörer i deras Säkerhetscenter.

Microsoft har sedan september 2011 kunnat peka på att de uppfyller Datainspektionens krav punkt för punkt vad gäller deras standardiserade personuppgiftsbiträdesavtal.

Microsoft Azure har uttryckligt klarat testet i ärendet angående Brevo

Office 365 har uttryckligen ansetts uppfylla Datainspektionens krav

Vad står i Microsoft Trust Center?

Security: We keep your data safe

Privacy: You own and control your data

For more than two decades, Microsoft has been a leader in creating robust online solutions

Compliance: We conform to global standards

Transparency: You know how your data is stored and accessed, and how we help secure it

Microsoft Azure is built on the premise that for you to control your own customer data in the cloud, you require visibility into that data. You must know where it is stored. You must also know, through clearly stated and readily available policies and procedures, how we help secure your customer data, who can access it, and under what circumstances. Don't take our word for it: you can review third-party audits and certifications that confirm how we meet the standards we set.

- **Maintain clear, constant visibility.** You know where your data is stored, who can access it, and under which conditions your data is accessed. You receive updates to any changes in our service operations policies.
- **Rely on strict access procedures.** Microsoft grants access to customer data to Microsoft engineers, to perform key tasks such as maintenance and upgrades, and subcontractors, to perform limited services. We use strict controls to govern access to customer data, assign the lowest level of privilege required to complete key tasks, and revoke access when it is no longer needed.

Learn more by reading Azure Transparency.

Nya EU dataskyddsförordningen

Gamla Dataskyddsdirektivet från 1995 (varje medlemsstat implementerar nationell lag)

Förordning (direkt som lag) ger harmonisering i EU för att skapa fri rörlighet av varor och tjänster
Moderniserad = Teknikneutral utan beskriver syfte och ändamål

Klar maj 2017, Träder i kraft 25 maj 2018

Vad skiljer den nya förordningen mot PUL?

Det mesta finns redan med i PUL. Det kommer dock att kosta mycket pengar att bryta mot förordningen.

Notifieringskrav inom 72h meddela incidenter till myndigheten. Även till registrerade vid hög risk för överträdelser.

Man måste kunna visa hur man efterlever kraven i förordningen (dokumentera)

Ökade rättigheter för de personer som registreras, inklusive rätt att kräva skadestånd och rätten att bli glömd

Överföring till Tredje Land

Överföring till tredje land: Förbjudet om man inte har stöd i förordningen

Tillåtet vid bl.a.

- Beslut från kommisionen (ex kommande privacy shield USA)
- Binding corporate rules (BCR)
- Standardavtalsklausuler
- Branschorganistationer kan få uppförandekod godkänd av mydigheten
- Godkänd certifiering
  - Kommer nog att få impact då det kommer att ge konkurrensfördelar
- Uttryckligt samtycke

Skadestånd

Skadestånd från ansvarige eller biträdet

Biträden och ansvarige kan vara solidariskt ansvariga och detta måste noga hanteras i avtalen (hur man senare fördelar ev skadeståndskrav)

Skadestånd

Upp till 2% av globala omsättningen eller upp till 10mEUR (det som är högst)

Exempel:

- Anlitat biträde som inte har implementerat tillräckliga tekniska/organisatoriska åtgärder
- Anlitat underbiträden utan tillstånd från ansvarige
- Brister i personuppgiftsbiträdesavtal
- Brister i upprättande av register över behandlingar
- Brister i privacy by design and by default
- Brister i uppfyllande av krav på risk- och sårbarhetsanalys

Skadestånd

Upp till 4% av global omsättning eller upp till 20mEUR (det som är högst)

Exempel:

- Bristande uppfyllelse av grundläggande principer, laglig grund eller krav på behandling av känsliga personuppgifter
- Bristande uppfyllelse av informationskrav, rätt till att bli glömd
- Överträdelse av krav på tredjelandsöverföringar

Vad bör man göra?

Exempel på rekommenderade åtgärder

- Gör GDPR till en ledningsgruppsfråga
- Inrätta en organisation för att tillse efterlevnad (ha någon person som är gatekeeper)
- Se till att rätt individer har adekvat kunskap om personuppgiftsreglerna

Kartlägg alla pågående personuppgiftsbehandlingar och kontrollera laglighet mot förordningen

Gör en risk och sårbarhetsanalys vid varje ny personuppgiftsbehandling