Genvägen till GDPR

Luleå Energi Arena, Live-restaurangen
Fredagen 4 maj kl. 11:30 – 13:00

I samarbete med Dataföreningen

DATAFÖRENINGEN

(bildkälla: https://toolstotal.com/)

Pasi Hautamäki

Pasi Hautamäki

Evangelist
Tieto, Business Consulting and Implementation
pasi.hautamaki@tieto.com

tieto

Table of contents

Snabb PRIMER

Vad?, När?, Hur?

tieto

Vad?, När?, Hur?

- **Denna månad 25 Maj, träder den nya europeiska Dataskyddsförordningen ikraft.**

- Den nya europeiska Dataskyddsförordningen har kallats för den **största it-omställningen på 20 år**.

- Ca **85 procent har ej inlett arbetet** och kommer inte kunna möta de nya kraven i tid, vilket innebär att man gör detta med en medveten risk, som kan stå en dyrt.

Hur kan en checklista se ut? (exempel)

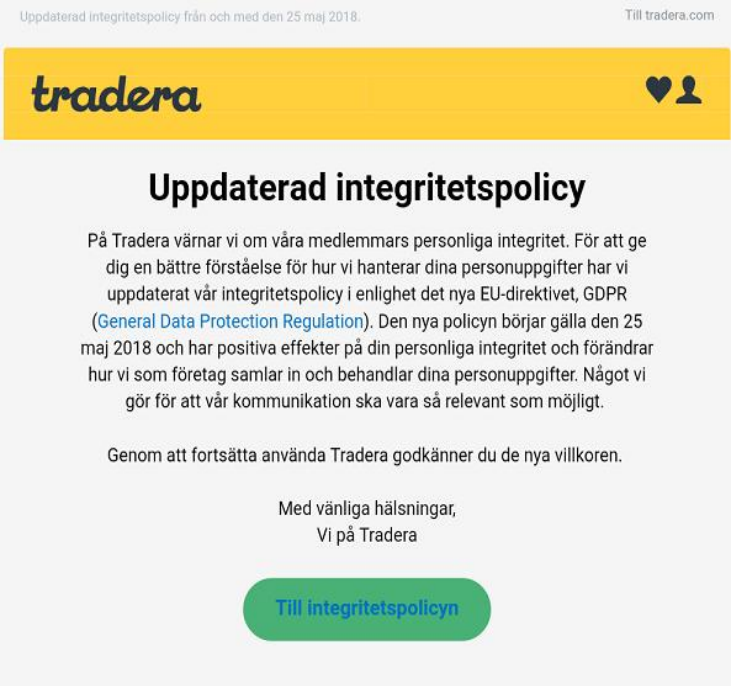
- ✓ 1. **Skaffa resurser** - Du behöver mandat och en budget som är förankrad i både styrelse och ledningsgrupp.
- ✓ 2. **Börja dokumentera** - GDPR ställer stora krav på dokumentation och att du hela tiden kan visa hur du har fattar beslut om personuppgiftshantering. Börja därför dokumentera alla delar av arbetet, inte bara själva hanteringen utan även processen på vägen mot GDPR-överensstämmelse.
- ✓ 3. **Samordna organisationen** - GDPR är inte en enskild fråga för it, juridik, stab. Hela organisationen ska med på tåget och någon behöver sitta i förarsätet och driva projektet framåt.
- ✓ 4. **Utse ansvariga** - Utse ett dataskyddsombud eller, om det inte är nödvändigt, en person som har organisationens dataskydd som sitt särskilda ansvar. Utse även ansvariga för genomförandet inom respektive avdelning.
- ✓ 5. **Kommunicera internt** - Alla medarbetare bör få veta vad som sker i och med att GDPR införs, varför och förordningens konsekvenser.
- ✓ 6. **Läs på principerna för behandling** - GDPR har sex grundläggande principer för hur personuppgiftsbehandling ska ske. Alla bör känna till dem och ha dem i åtanke i resten av processen.
- ✓ 7. **Inventera personuppgifter** - Vilka personuppgifter skapas, lagras och hanteras i verksamheten? Detta gäller även osorterade data som e-post och liknande eftersom GDPR till skillnad från PUL inte ger undantag för sådana.

*Freja eID info

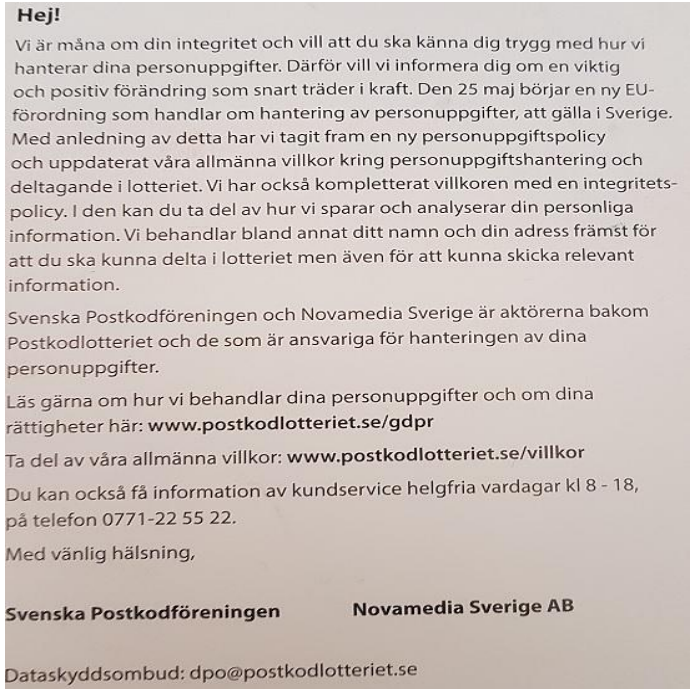
- ✓ 8. **Stäm av ändamålen** - I vilka syften skapas uppgifter och hur lagras och hanteras personuppgifterna i databaser samt i osorterad form?
- ✓ 9. **Kartlägg systemen** - Var finns personuppgifterna lagrade, I interna system eller i molnet?
- ✓ 10. **Avgör på vilka lagliga grunder uppgifter behandlas** - Inga personuppgifter får lagras ”för att de kan vara bra att ha”. Du behöver en laglig grund för varje behandling. Försök hitta en stark och stabil grund.
- ✓ 11. **Ta det säkra före det osäkra** - Gallra i de fall du hittar personuppgifter som har samlats in på lösa grunder, till exempel mot samtycke men där du saknar dokumentation av lämnade samtycken, sålla bort uppgifter som du inte kan visa att du lagrar på en laglig grund.
- ✓ 12. **Kontrollera säkerheten** - Högre krav ställs på it-säkerhet för lagrade personuppgifter. Utred om säkerhetslösningar behöver uppdateras eller bytas ut. (2FA, IAM, Freja eID* mfl)
- ✓ 13. **Granska alla avtal** – Avtal behöver ses över så att inte personuppgifter lagras felaktigt eller behandlas på fel sätt. Ingen utomstående får behandla uppgifter du har ansvar för utan att skriftligt avtal.
- ✓ 14. **Sätt upp nya rutiner/checklistor** - Personuppgifter som organisationen skapar och förfogar över kan behöva hanteras enligt nya rutiner under GDPR.
- ✓ 15. **Utbilda medarbetare** - Ordna interna GDPR-kurser för de roller som kommer att hantera personuppgifter i organisationen.

Utmaningen med samtycke, gör rätt!

- Mindre bra exempel



- Mycket bra exempel



Sen på bollen, och du behöver en genväg?

- Kryptering eller pseudonymisering nämns 19 ggr EU-förordningen (EU-GDPR)

PDF File

- Krypterat data är inte data, men du måste kunna bevisa att endast du har tillgång till nycklarna
- Tieto har tagit fasta på detta och skapat en tjänst som bygger på kryptering

Tjänstens fördelar

- *Skydd av individens/medborgarnas personuppgifter*
- *Efterlevnad av kraven i dataskyddsförordningen*
- *Behåll lagrings- och backuprutiner oförändrade*
- *Strikt åtkomstkontroll, skyddar även mot administratörer hos molntjänstleverantörer*
- *Slippa rapporteringsskyldighet (av incident) till myndighet (DI) och medborgare*
- *Policyhantering (regler), sortering av personuppgifter efter risk*
- *Loggning och revision*
  - *Bland det viktigaste är att skydda personuppgifterna och kunna sortera dessa efter känslighetsgrad och styra vilka system och användare som får komma åt dem, samt att i efterhand kunna bevisa vilka som haft åtkomst till uppgifterna.*
  - *Lika viktigt är det att säkerställa att obehöriga användare och system, inklusive hostingföretag och molntjänstleverantörer, inte kan komma åt personuppgifter även om organisationen/kommunen litar på dem för att tillhandahålla en kritisk tjänst.*

Tjänstens mervärde

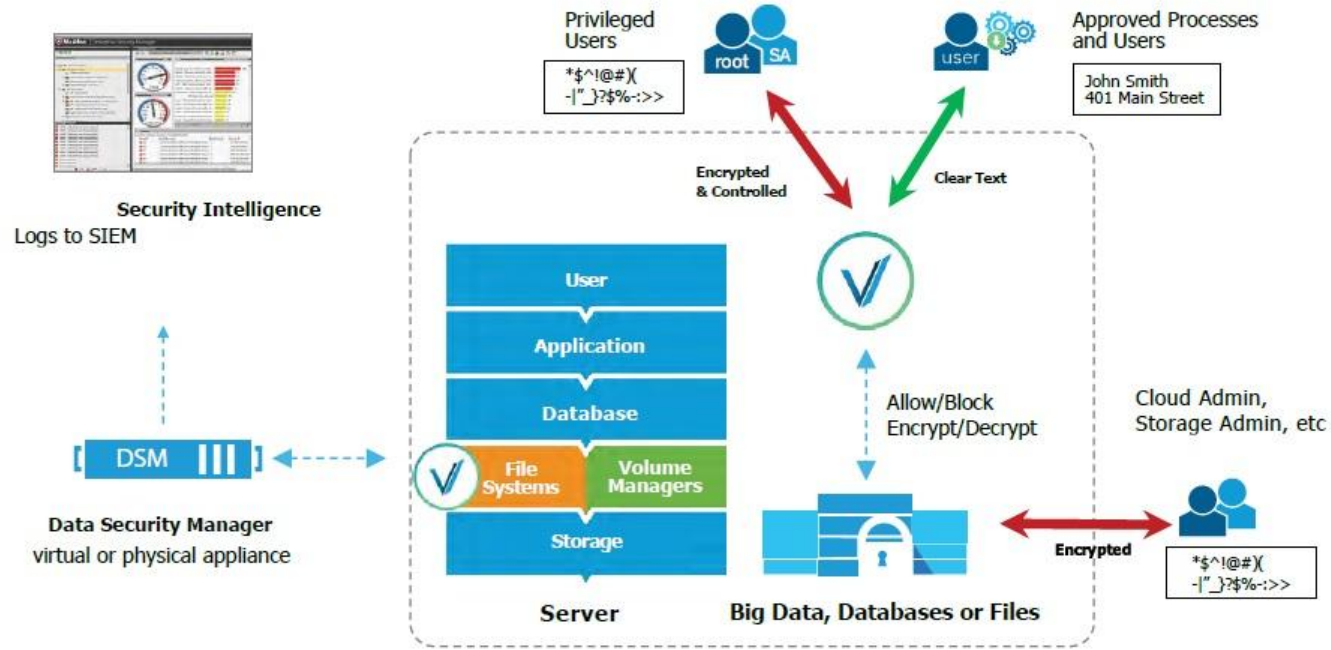
- *Transparent skydd av lagrade personuppgifter som tjänst och följ dataskyddsförordningens krav från **dag 1.***
- *Ni styr själva över era regler för uppsättningen och över de nycklar som kan låsa upp det skyddade datat. Vi rullar ut mjukvaruagenter till de servrar ni vill att vi skyddar.*
- *Agenten lägger sig under applikations- och databasnivå och sköter kryptering och av-kryptering mellan applikation och datalager. Det krävs därför ingen integration, därav namnet transparant.*
- *Organisationen/Kommunen måste endast avsätta 1-2 mandagar åt att bestämma vilka servrar som ska skyddas och vilka regler som ska gälla för dem, men vi tillhandahåller standardmallar som ni kan komma igång med. När datat väl är skyddat och ni kan visa att endast rätt användare och system kunnat komma åt uppgifterna i klartext, är ni inte längre skyldiga att anmäla eventuella incidenter där det lagrade datat kommit bort eller stulits, eftersom detta inte längre anses känsligt.*

Tjänstens prissättning

TIETO TRANSPARANT DATAKRYPTERING

- 7/24/365 tillgänglighet SLA 99,5 %
- Central nyckelhantering (molntjänst) med hög tillgänglighet (HA)
- 5 stycken server agenter
- Implementation, Kort tid - oftast dagar
- 1 års bindningstid
- *Kostnad* ***19.995 sek/månad***

Övergripande bild av tjänsten



Faktaruta om Freja eID

Freja eID gör följande som är viktigt för att vara GDPR READY: (se även www.frejaeid.com – Officiell hemsida)

Tjänsten är kvalitetsmärkt av e-legitimationsnämnden, dvs att IT säkerheten, accesskontrollerna, incidenthanteringen mm. är granskade, stickprovskontrollerade och godkända. E-legitimationsnämnden likställer Freja eID legitimationen med en fysisk ID handling (LOA3). Detta gör att online tjänster kan lita på att det endast släpper in rätt person. Detta är liksom grunden till skydd av personuppgifter.

Det krävs dual-control (två personer i förening) för alla kritiska actions och processer som på något sätt kan skapa risker för datasäkerheten, detta är resurskrävande men ett krav för att inte ”single points of failure” ska vara möjliga.

Alla kritiska actions loggas och signeras kryptografiskt så att de inte går att ändra i efterhand. På så sätt kan man gå tillbaka i tiden och ”forensiskt” undersöka vad som skett, om en incident ändå inträffar. Detta är en viktig del i GDPR.

Alla personuppgifter krypteras. Kryptering är inte ett absolut krav enligt GDPR om inte personuppgifterna är känsliga, men Freja eID behandlar alla personuppgifter som känsliga.

Med Freja eID-appen kan man inhämta ett juridiskt bindande **samtycke** från individen för all behandling av personuppgifter samt att i "Mina Sidor" kan individen se alla transaktioner, inloggningar och underskrifter som denne genomfört. Hen kan se alla förlitande parter (service providers) som är kopplade till Freja eID och **ge eller vägra samtycke till att en viss aktör får tillgång** till dennes **personuppgifter** och eID.

Jämför detta med BankID där bankerna bestämmer vilka tjänster jag som individ ska kunna logga in på. Genom att BankID kan användas på tusentals tjänster exponerar detta individen för att dennes personuppgifter hamnar på drift, med Freja eID måste individen först ge sitt samtycke.

I "Mina Sidor" kan individen också se vilka personuppgifter som lagras om hen. När individen efter 25 Maj loggar in till en tjänst för att få reda på om vilka personuppgifter som finns lagrade om denne, eller önskar bli ”bortglömd”, eller vill få uppgifterna utlevererade i maskinläsbar form, då är det extra viktigt att det är en godkänd e-legitimation som används för detta. En oberoende instans som går i god för identiteten. Det kan man inte åstadkomma med endast 2FA/MFA teknik.

Passa på och nyttja GDPR rätt

Pasi Hautamäki

Evangelist
Tieto, Business Consulting and Implementation
pasi.hautamaki@tieto.com