Big Findings concerning Personally Identifiable Information

ie. what you have to consider when you gather and process Big Data!

Timo Seppänen, Ineo Oy, 20170517

FACT-BASED ★ ★ ★ GDPR COMPLIANCE | INEO

Top three GDPR findings

- Do not rely on IS design models & methods!
- Your history is Your Enemy!
- Beware of circumstantial dependencies!

Don’t rely on IS design models & methods!

PII Lifecycle Management

- Poor life cycle management models/ methodologies and/or applying of them in IS design
- Undefined/-managed Retention and Retention Periods of Information
- Disposal of Information is technically difficult, in some cases, almost impossible

PII Architectural Consistency

- GDPR requires a logical view of PII on an Enterprise level, System-/Model-/Application internal concepts/views are insufficient
- Poor key mastering principles results in unnecessary GDPR contamination of unrelated information

Your history is Your Enemy!

Undisposed or outdated information

- Old inactive and/or archived PII are in breach of the regulation and require
  - documentation of the retention principles,
  - obtaining retention justification or
  - disposal of the information
- Un-synchronized maintenance routines in a multi-system landscape result in insufficient disposal efforts

Undisposed or outdated information

- Applications/Reports do not show inactive information, leaving the maintainers unaware of PII breaches

Beware of circumstantial dependencies!

Unintended contamination

- Incomplete system behaviour / use-case support leads to PII being entered into un-wanted information containers
- Non-PII becomes PII due to logical and/or temporary integration of two seemingly un-related systems (ie. IOT)
- Tissue –specimen, fingerprint etc. are, as such, a PII carrier and might contaminate unrelated databases / systems

Unintended contamination

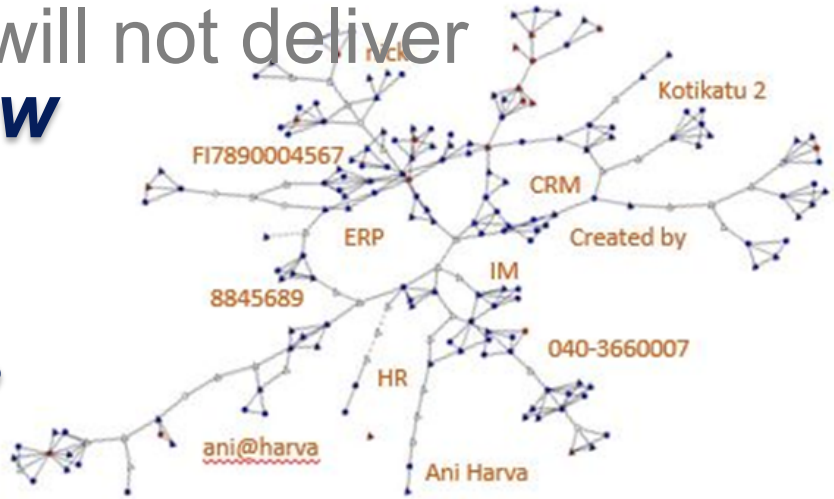
- A too concise profiling or sample can lead to PII becoming special PII
- End-user portals can become GDPR breach generators as the Data Subject may intentionally or unintentionally enter undesirable PII into the portal

About the GDPR Analysis

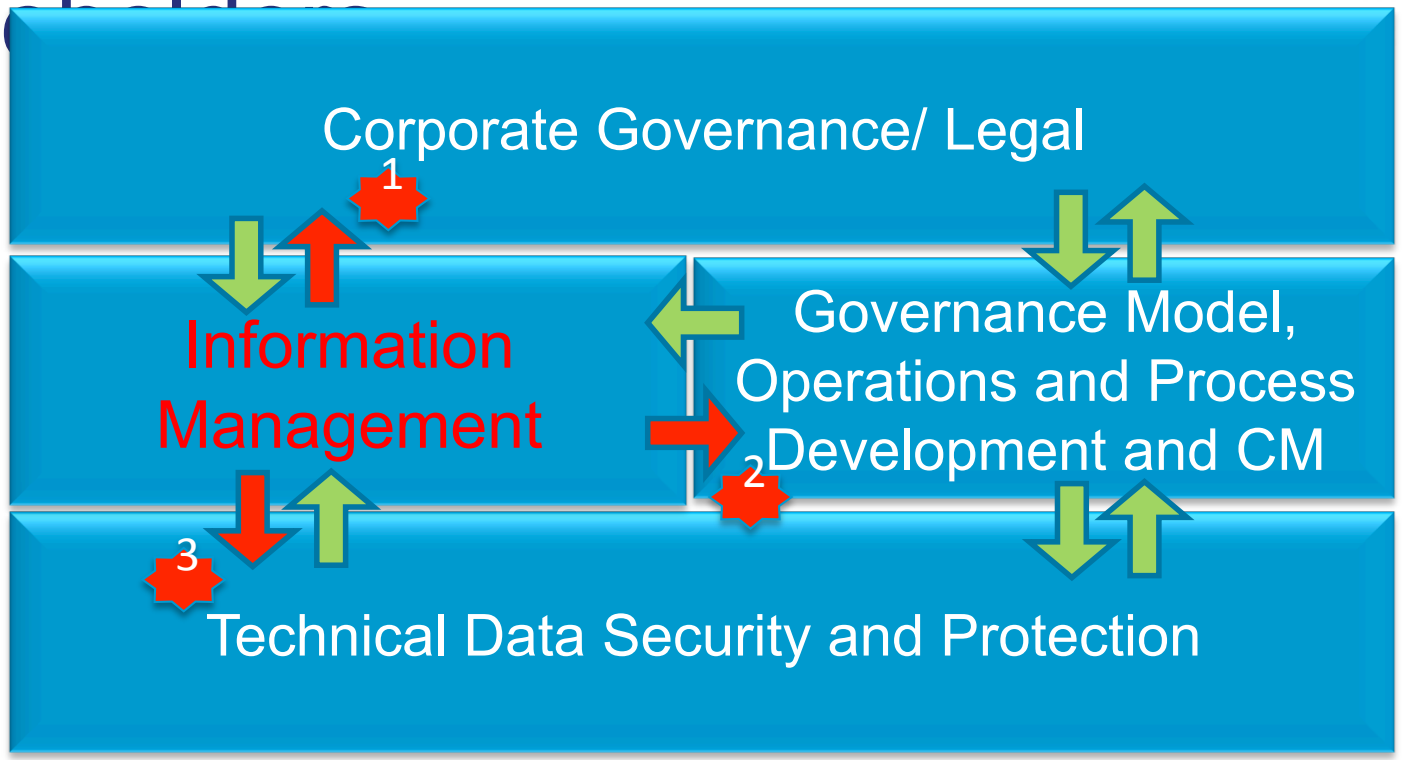
GDPR compliance is achievable only with hard facts about PII in your systems

- GDPR introduces new requirements for Personally Identifiable Information (PII) that was previously legitimately outside of the scope of the regulation.
- Reaching GDPR compliance requires locating the actual scope of the PII – risk management and governance alone will not deliver compliance.

Do you know the exact locations of your PII?



The highlights of Ineo's GDPR Analysis addresses your internal stak



1. **Presents the actual scope of the GRC issues & governance needs**
2. **Builds the service foundation enabling the Data Subject to exercise his/her rights**
3. **Highlights the technical & security topics to be addressed**

Seal of Excellence

FACT-BASED ★ ★ ★
GDPR COMPLIANCE | INEO