Architecture Principles for Data Privacy of Cloud-based Medical Device Services

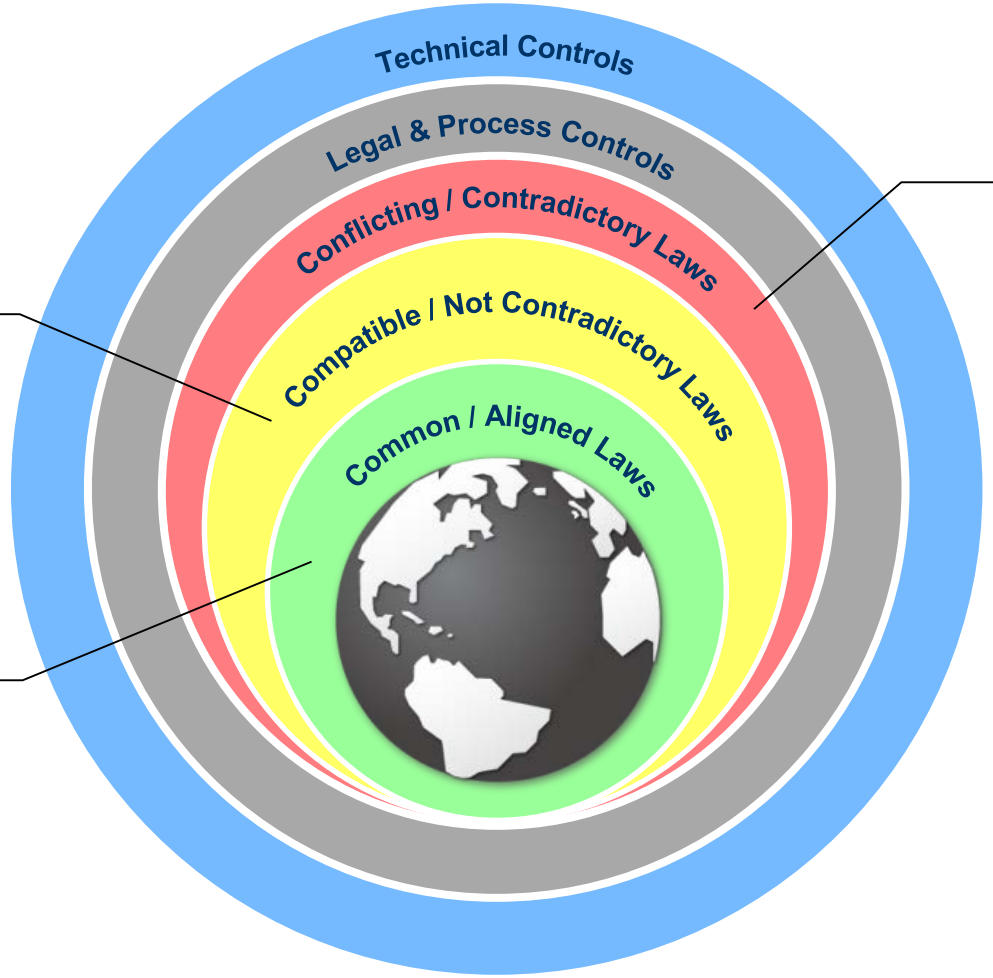
Dr. Andrzej J. Knafel

Data Protection Laws

Architecture for Selected Technical Controls of Data Privacy

Conclusions

Data Protection
Overview of laws and controls dependencies



Examples:
- Security Certifications
- Anonymization

Examples:
- Data Portability
- Audit Trail

Examples:
- Opt-in vs. Opt-out
- Data Residency in Country vs. Controlled Data Transfer
- Access for Law Enforcement

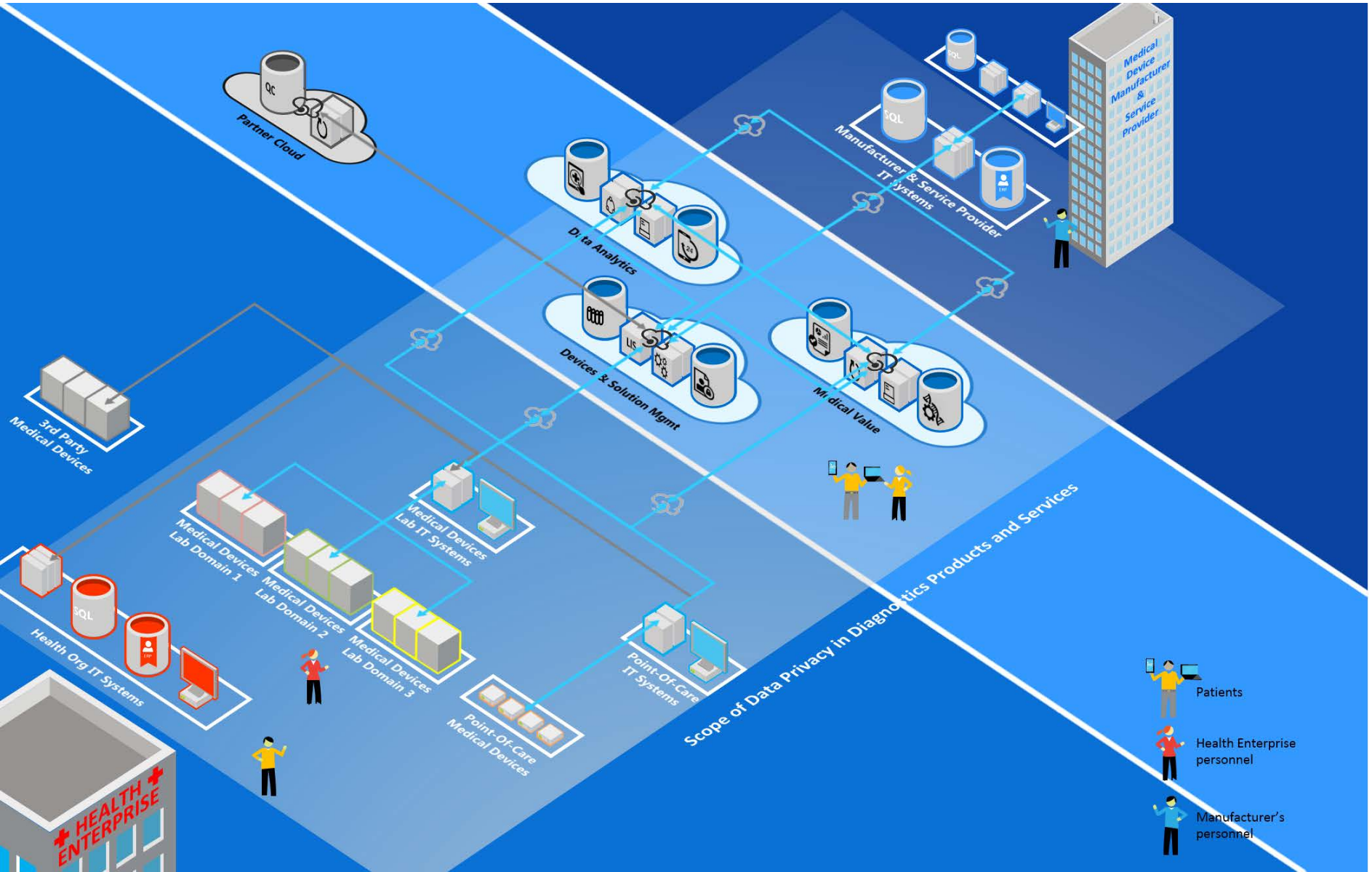
Data Protection
European Union General Data Protection Regulation (GDPR)

- In effect starting on 25 May 2018
- Processing of “personal data” in the context of the activities in the EU
- Processing data of “data subjects who are in the Union”
- GDPR may apply to manufacturer or service provider when:
  - has legal presence in the EU
  - offers goods and services to EU residents
  - monitors the behavior of EU residents, e.g. websites and mobile apps tracking digital activities of visitors
  - has employees in the EU

Data Protection
GDPR in a nutshell

Broader Scope	Rights of Individuals	New Provisions	Risk Based Approach
• Harmonization: one continent – one law • Consent: to be unambiguously given for each specific purpose; withdrawal any time • Special data categories: biometric and genetic • Expanded definition of Personal Data • Detailed and elaborate provisions on Supervisory Authority	• Right to Access: Data Subjects gets broader information • Right to Erasure: conditions for and against enforcing • Right to Restrict Processing: rationales and consequences of enforcement • Automated Decision Making incl. Profiling: Data Subject can obtain human intervention, explanation and challenge the decisions • Data Portability: Data Subject right to receive personal data in structured, commonly used and machine readable format or have them directly transmitted to other Data Controller	• Data Transfer to third Countries: alternate provisions in absence of adequacy; Effective Safeguards, Binding Corporate Rules • Fines: high fines for non-compliance • 18 new definitions • Increased responsibility and accountability of Controllers and Processors: maintaining detailed Records of Processing Activities; obligation to report data breaches without delay to Supervisory Authority and Data Subject • Compensation and Liability: by Controllers and Processors	• Data Protection by Design: accounting for privacy risk by implementing appropriate technical and organizational measures throughout the process of establishing a new product or service • Data Protection by Default • Data Protection Impact Assessment • Data Protection Officer

Medical Devices and Services for Diagnostics
Scope of Data Privacy



Data Subjects to be protected

- Patients
  - hospitalized
  - in ambulatory care
  - self-managed
- Health Enterprise personnel
  - operators of medical devices
  - operators of IT systems
- Manufacturer's personnel
  - operators of IT systems
  - service & support

Data Protection Laws

Architecture for Selected Technical Controls of Data Privacy

Conclusions

Architecture Principles for Data Privacy
Example of a common challenge …

Scenario

1. ACME architected system/service used at clinical lab XYZ and underlying GDPR and GxP regulations is operated by a group of individuals employed by XYZ (remark: regulations, like GxP mandate Audit Trail)
2. One of the operators leaves XYZ and demands that his/her data will be erased from all systems related to his/her work

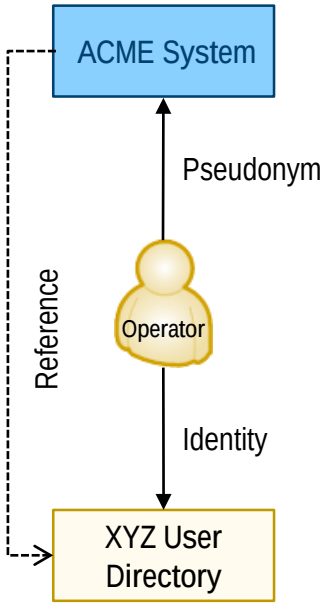
Challenge

– What is the easiest and cost efficient way to offer the compliance with the GDPR article 17? (Erasure of Personal Data)

Suggestion

– Design the system to use pseudonymized* (tokenized) “operator id” in login, audit trail and other logs (GDPR article 20).

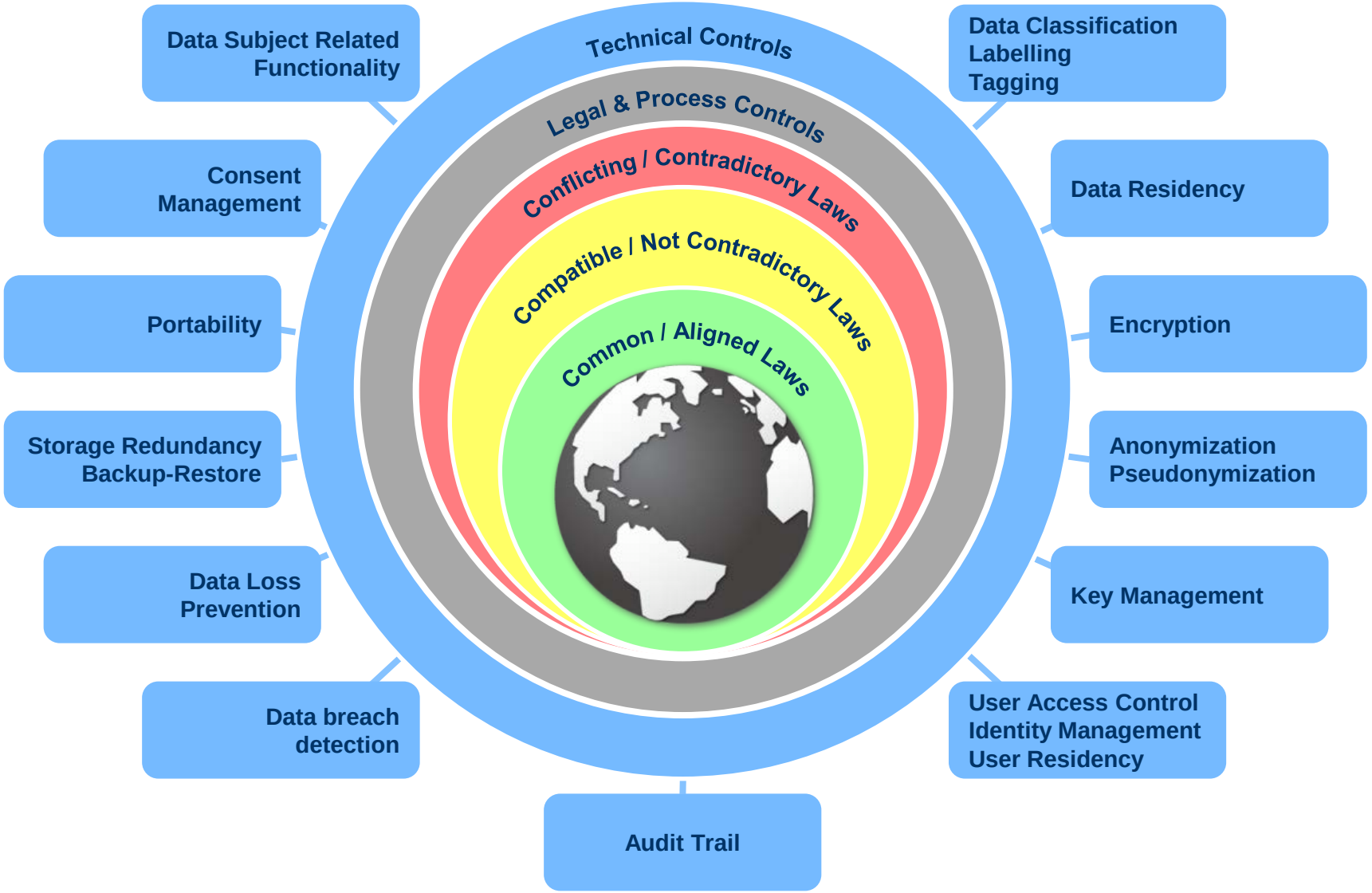
– Do not capture and store any Personal Data of the operator (name, e-mail, …), but instead refer to the user directory of lab XYZ



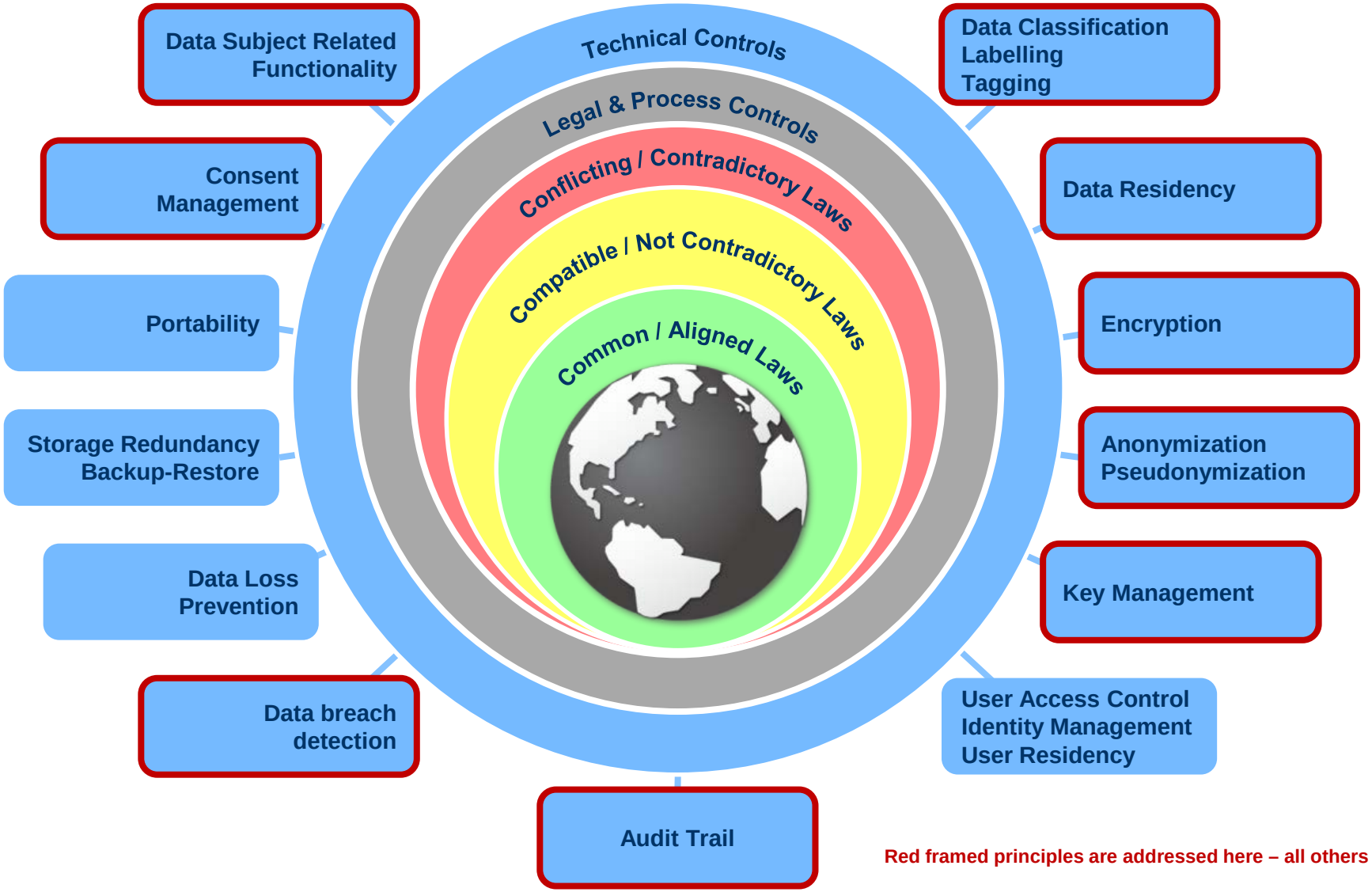
***** pseudonymized - GDPR definition, Article 3(5)

‘pseudonymisation’ means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information,
provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Architecture Principles for Data Protection
Overview of Technical Controls areas



Architecture Principles for Data Privacy of Cloud Services
Selected examples of Technical Controls



Red framed principles are addressed here – all others may be available on request.

Architecture Principles for Data Privacy of Cloud Services
Example: Anonymization / Pseudonymization [GDPR article 6, 25, 32]

1. Data, which is neither classified as “Public”, nor provided with consent for the specified purpose, and is intended for use as the source for data analytics or aggregation, should undergo anonymization utilizing techniques supported by the CSP technology and assessment practices published in “Anonymization techniques 0829/14/EN WP216”.

Anonymization is the preferred solution over pseudonymization.

2. **Avoid using Pseudonymization with the records of mapping the pseudonyms to the identity in the scope of the same solution**.

Pseudonymization is not a failsafe approach per the data protection requirements, because pseudonymized data can be re-identified to a specific natural person through various organizational and technological means.

3. Unstructured data elements may contain identifiable information and it should be treated as Personal Data.

Pseudonymization should be preferred over managing the identity of the Data Subject.

Architecture Principles for Data Privacy of Cloud Services
Example: Data Classification – Labelling / Tagging [GDPR article 10]

1. Each data item category should be classified and correspondingly labelled.
2. Multiple labels can be applied to individual data items.
3. Use labels aligned / standardized within your industry or organization.
4. In objects with a combination of labels of various classes, the strictest label shall be applied.
5. Labels:
   a. Confidentiality level
      i. Public
      ii. Internal
      iii. Confidential
      iv. Secret
   b. Location containment
      i. Open worldwide
      ii. Keys Storage in Accepted Region
      iii. Keys and Data Storage in Accepted Region
   c. Purpose of use
      i. Medical Value
      ii. Lifestyle Advice
      iii. …

Use automatic data classification service.

Examples

AWS Macie
A service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Amazon Macie recognizes sensitive data such as personally identifiable information or intellectual property.

https://aws.amazon.com/macie/

Google DLP API

DLP API provides fast, scalable classification and redaction for sensitive data elements like credit card numbers, names, social security numbers, US and selected international identifier numbers, phone numbers and GCP credentials.

https://cloud.google.com/dlp/

MS Azure DgSecure or SQL Threat Detection

DgSecure detects, audits, protects, and monitors sensitive data assets and is optimized for HDInsight and other Hadoop Distributions including Hortonworks, Cloudera, and MapR.

https://azuremarketplace.microsoft.com/en-us/marketplace/apps/dgsecure.dgsecure

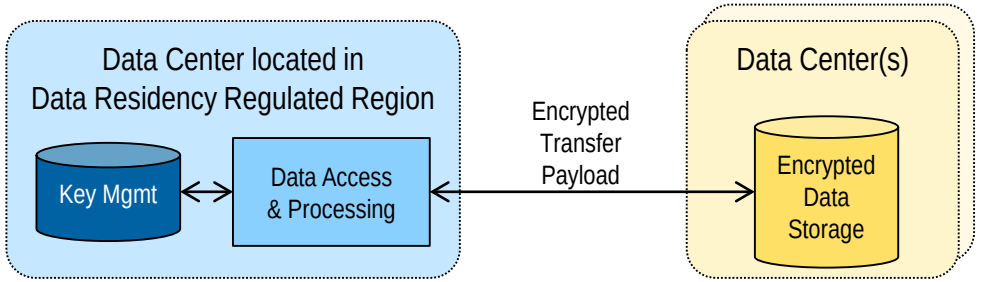
https://docs.microsoft.com/en-us/azure/sql-database/sql-database-threat-detection

Architecture Principles for Data Privacy of Cloud Services
Example: Data Residency

1. **Personal Data originating in a data privacy regulated region should not leave that region**
   a. Utilize Data Centers of the CSP or their partners geo-located within the region accepted by the regulatory and statically assign origin to the storage target
   b. If no CSP Data Centers are available in the accepted region or other constraints occur: use private cloud deployment for storage of the Personal Data (PD).
2. If containment within the data privacy regulated region where the Personal Data originated is not possible, then that data **SHALL not leave** that region **unencrypted**
   a. Use encryption with localized key management and access control for storage of the data outside of the region.
   b. Whenever processing of clear text data is necessary, this processing, including the data decryption, shall be conducted in the accepted region.

If permitted by the regional authority:

use encryption with localized key management, i.e., change the "data residency" requirement into "key residency" requirement.



If "key residency" principle is not permitted:

use micro-segmentation, e.g., VPC, IAM, Network ACLs, Security Groups, Key/Certificate Management, to localize data in the regulated region.

Architecture Principles for Data Privacy of Cloud Services
Example: Key Management [GDPR article 29]

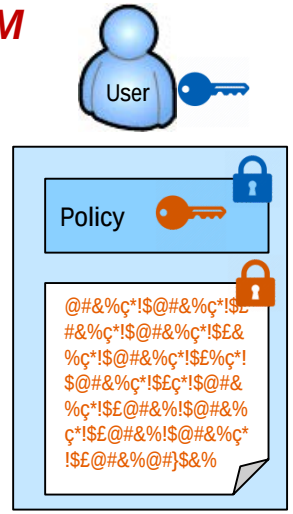
1. **Key management** shall
   a. be **assignable to** the organization in the role of **Data Controller**
   b. support keys from multiple sources
   c. **enable storage of the keys** in locations **within the region** accepted by the regulatory of the data origin country (key-store residency)
   d. support HSM protected key storage if requested
   e. **enable withdrawal** of the effective key control from the CSP.
2. Keys used for authentication and access control should **per default be valid for a limited time and expire** after reaching that limit.
3. If feasible, use Customer Managed Keys (CMK) practices to give control to the controller of the data source organization.
4. If feasible, use **Information Rights Management (IRM)** technologies whenever supported by the CSP.

Use key management functionality provided by Cloud Service Providers

- ***highly available, fully managed service to generate, store, enable/disable, delete symmetric keys***
- ***Hardware Security Module for key storage of sensitive / regulated data***
- ***regionalize key storage & key management***

Some Cloud Service Providers support IRM

- ***the data is encrypted at the application level and includes a policy that defines the authorized use for that document***
- ***at access of the protected document by a legitimate user or an authorized service, the data in the document is decrypted and the rights defined in the policy are enforced***



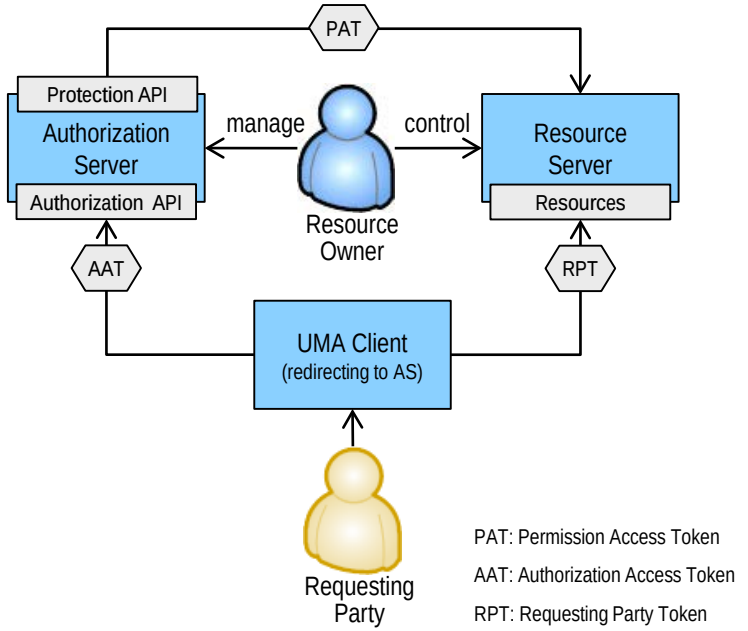
Architecture Principles for Data Privacy of Cloud Services
Example: Consent Management [GDPR article 12, 13]

1. Design consent objects to **differentiate between metadata** (consent id, version, purpose …) **and Data Subject consent attributes** (collector, time-stamp, expiration …).
2. The consent metadata should **support real-time decisions** for applications accessing the data requiring consent.
   The matching of the consent metadata with the data labels based on Data Classification fosters this objective.
3. Design **self-service consent management** which enables the Data Subject to easily opt-in / revoke / restrict the consent.
   The consent object attributes should be easy to understand for the Data Subject.
4. The consent management should per default use the principle of **least privilege** needed to make application decisions.
5. The consent management should support **automatic "opt-out" after expiry**.
6. The **consent transaction shall be audited**.

Whenever available, use existing APIs for accessing and transferring the consent data.

Consider: Health Relationship Trust Profile for User Managed Access

http://openid.net/specs/openid-heart-uma-1_0.html
implementation examples:
https://kantarainitiative.org/confluence/display/uma/UMA+Implementations



Architecture Principles for Data Privacy of Cloud Services
Example: Data Subject Specific Functionality [GDPR article 14,15,16,17]

The following functionality related to the Data Subject should be supported by the architecture:

1. **Access by the Data Subject** to both the Personal Data and information related to processing of this data, data recipients, data transfers, and subsequent rights. *Article 14, 15*.
2. **Rectification / correction** and update of Personal Data. *Article 16*.
3. **Erasure of Personal Data** if no regulatory defined specific conditions prohibit it. *Article 17*.

The "Access by the Data Subject to … information related to processing of this data, data recipients, data transfers …" can be achieved through functionality implementing an analysis of the Audit Trail logs.

If individual encryption keys are used for a specific Data Subject or related data fields, then the "Erasure of Personal Data …" may be achieved by deleting of the encryption key.

Architecture Principles for Data Privacy of Cloud Services

Example: Audit Trail [GDPR article 30]

1. Utilize CSP functions of the audit trail collection and management. Ensure that events are captured relating to Personal Data (PD) processing by extending these mechanisms when necessary.
2. Ensure the integrity of the audit trail records by using the means provided by CSP or applying digital signatures, when applicable.
3. Safeguard immutability of audit trail records – enable deletion only by the specifically designated privileged user - prevent deletion by a privileged user.
4. Encrypt the audit trail data to protect data privacy in case of included PD.
5. For transfer of audit records between systems should use the SYSLOG-TLS protocol, and the audit records format according to the XML Schema provided in “Digital Imaging and Communications in Medicine standard”.
6. Use a synchronized time, e.g., single reference time source to ensure proper event correlation.

IAM / UAC events

- *Registration Request of a new User*
- *Creation/Modification/Deletion of a User Account*
- *Modification of User Access Rights / Security Roles (incl. disabling of Access)*
- *User Login/Logout*

Audit Trail events

- *Export/Import of Audit Records*
- *Read Access to Audit Records*
- *Deletion of Audit Records*

Personal Data events

- *Creation / Submission of a PD Data Record*
- *Modification / Update of a PD Data Record*
- *Deletion of a PD Data Record*
- *Query / Access to PD Data Record*
- *Transfer of PD Data Record*
- *Creation of a Consent Data Record*
- *Modification (incl. any restrictions) of a Consent Data Record*
- *Revocation of a Consent Data Record*

System operation events

- *System Start*
- *System Stop*
- *Emergency Access Start/Stop*
- *Node Authentication Failure*
- *Significant Change in Connection Status of a Device*
- *System Configuration Change*
- *Switching Audit Recording On/Off*
- *Modification of Security Attributes of an Object*
- *Use of a Restricted Function*
- *Security notification (e.g., automatic detection of a potential data breach)*

Architecture Principles for Data Privacy of Cloud Services
Example: Encryption [GDPR article 5, 6, 25, 32, 34]

1. **Per default encrypt all data in transfer / in motion**
   a. **Authenticate sources & destinations** using the cryptographic mechanisms
      i. Provided by the ITSP or
      ii. If the ITSP solution does not fulfil state-of-art crypto strength or the cost of this service is high, consider implementing X.509 certificate based authentication
   b. **Encrypt payload but supply metadata in clear text** including origin information and data classification labels enabling proper routing
   c. For data classified as “Secret” consider additionally end-to-end encryption
2. **Encrypt data at rest**
   a. Use state-of-art cryptographic means provided by the CSP.
   b. If feasible use Format-Preserving Encryption (see NIST Special Publication 800-38G “Methods for Format-Preserving Encryption”)

Current minimum crypto strength:

- ***Asymmetric -- RSA key length: 3072, DH: 3072 and ECC: 256***
- ***Symmetric -- AES-256 cipher and SHA-256 cipher.***
- ***Transport -- TLS version 1.2***

Consider that changes in encryption strength may require re-encryption or additional security envelopes.

Architecture Principles for Data Privacy of Cloud Services
Example: Data Breach Detection [GDPR article 33, 34]

1. Apply state-of-art Data Loss Prevention (DLP) capabilities provided by the CSP to **proactively detect** that data security has been breached.
2. Apply **analytics and monitoring** capabilities of the CSP (e.g. Machine Learning) to detect the data breach
   - Communication analytics
   - Monitoring of privileged user accounts
   - Monitoring of other suspicious behaviours
3. Ensure that the **information about which PD data records have been breached, is included in the detection**.
4. Ensure **push notification** technology provided by the CSP is used to **alert** the corresponding **Data Controller** organization or individuals.
5. If possible, **stop the data breach automatically**.

Example of DLP are Cloud Access Security Broker (CASB) solutions.

Monitoring of anomalous behavior in the cloud is available by 3rd party technology too.

The data breach detection should start the notification process (e.g., within a 72 hour window as per GDPR), therefore the alert should be timely received by the appropriate person, e.g. e-mail or messaging service.

Data Protection Laws

Architecture for Selected Technical Controls of Data Privacy

Conclusions

Architecture Principles for Data Privacy of Cloud Services
Conclusions

1. Despite differences of world data protection laws, architecture for common “technical controls” can be designed.
2. EU GDPR is a good starting point to architect the technical controls.
3. Popularity and adoption of cloud for transfer, storage and processing is growing rapidly.
4. Data privacy support by cloud services is growing, (e.g., data classification service, IRM)
    a. consider using existing cloud services in your design,
    b. demand changes (e.g., high granularity consent management service based on standard APIs).

Doing now what patients need next