tmforum
connecting digital ecosystems

Catalyst Pitchback

GDPR Compliance using Qiy Scheme

Companies

Champion Confirmed	Champion Tentative	Participant Confirmed	Participant Tentative
Vodafone		Qiy Foundation	IBM
Orange		UXP Systems	Accenture
			Telefonica

We are still looking for:

Problem Statement (one-liners)

- As a Data Controller or Processor
- I need to empower Data Subjects with solutions to that they can realise their rights to data portability, right to be forgotten, …
- So that I can be compliant to GDPR requirements
- To do this, I need innovative solutions and interoperability with other CSP or third parties
- I know I am successful when I manage to do this and develop new business at the same time

Problem Significance/ Market Drivers

Why is this an important problem to solve?

Accountability and Demonstrable Compliance

- **Privacy by Design** –ensure privacy is baked into the design of products and services (instead of an afterthought).
- **Data minimization** – processing only data that is necessary.
- **Consent** – Parental approval of Minor's consent
- **Data management:** Records of what data and how is being processed, by whom, where. Controls to make rights and obligations effective.
- **Supplier management** – selection, assurance, data protection and security agreement.
- **Security for privacy** – technical and organisational security measures to protect data, anonymisation and pseudonymisation.
- **International data transfer compliance**

Rights of individuals (e.g. Users, employees)

- **User Transparency** - informed about processing of personal data
- **Choice** - Explicit, revocable consents, e.g. sensitive personal data
- **Right to know** what data is actually processed
- **Right to object** to automated decision making, profiling
- **Right to be forgotten** - deletion of personal data
- **Data portability** – Right to take information to a different organisation
- **Breach notification** in case of data breach which may seriously impact the individual

Obligations towards regulators

- **Breach notification** to regulator (within 72 hours)
- **Data protection officer** to oversee implementation of controls, reporting to highest level of management
- **Assessment** to all High Risk data processing
- **Prior consultation with the regulator** in case of high risk processing of personal data (Risk remains high after mitigations have been implemented)

Powers of regulators

- **Investigations**, related information requests (cost of remediation)
- **Orders to comply** with the law
- **Orders to delete data** which was unlawfully collected
- **Warnings**
- **Fines** up to 4% of annual Vodafone Group global turnover
- **Comes effective 25th May 2018!!**

Use-cases addressed in the catalyst

- 1. Onboarding
  - a. Install Dappre app, create a QR code
  - b. Go to the CSP portal and scan the QR code
  - c. Pre-populate Qiy with personal information
  - d. Using OpenID connect (mentioned by Bram to John of UXP)
- 2. Giving consent to share personal data (part of onboarding)
- 3. Data Portability example
- 4. Audit trail (historical log of who requested what and when, so if it's challenged)
- 5. User Dashboard (transparent access to PII)
- 6. Right to Be Forgotten
- 7. Parental Approval

Simplifying GDPR compliance

tmforum

UXP Systems

User Permissions Dashboard

RESTful APIs

Regulator, Operator, DPO Audit API (ULM)

User Privacy Management

Permissions API
Provisioning API

ORANGE | **VODAFONE** | **TELEFONICA**

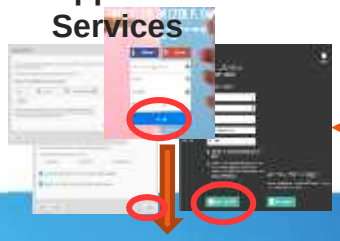
Service Provider 1 ↔ Service Provider 2 ↔ Service Provider 3

OnBoarding

Provision a Service
Send User Permissions

Application Service Simulator

Application Services

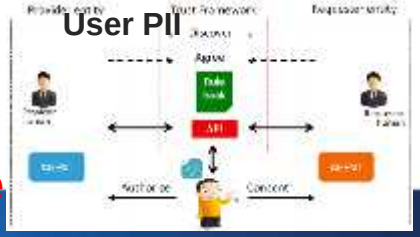


OTT Appls

OpenID

QiY Trust Scheme

Distributed User PII



Ideas for Innovation

What new areas do you plan to explore?

- *OpenID and Privacy Management APIs*
- *Communication between operators for data portability (format, APIs, …)*
- *Using network solutions instead of platform solutions*