Data Protection Office and Privacy by Design/by Default for Privacy Flag Project

Luca Bolognini – Italian Institute for Privacy (IIP)

Privacy Flag Project Enabling Crowd-sourcing based privacy protection for smartphone applications, websites and Internet of Things deployments

Medice cura te ipsum: how to deal with privacy and data protection compliance in a Privacy-as-a-Service project?

- Establishing a **Data Protection Office** with the collaboration of all Partners

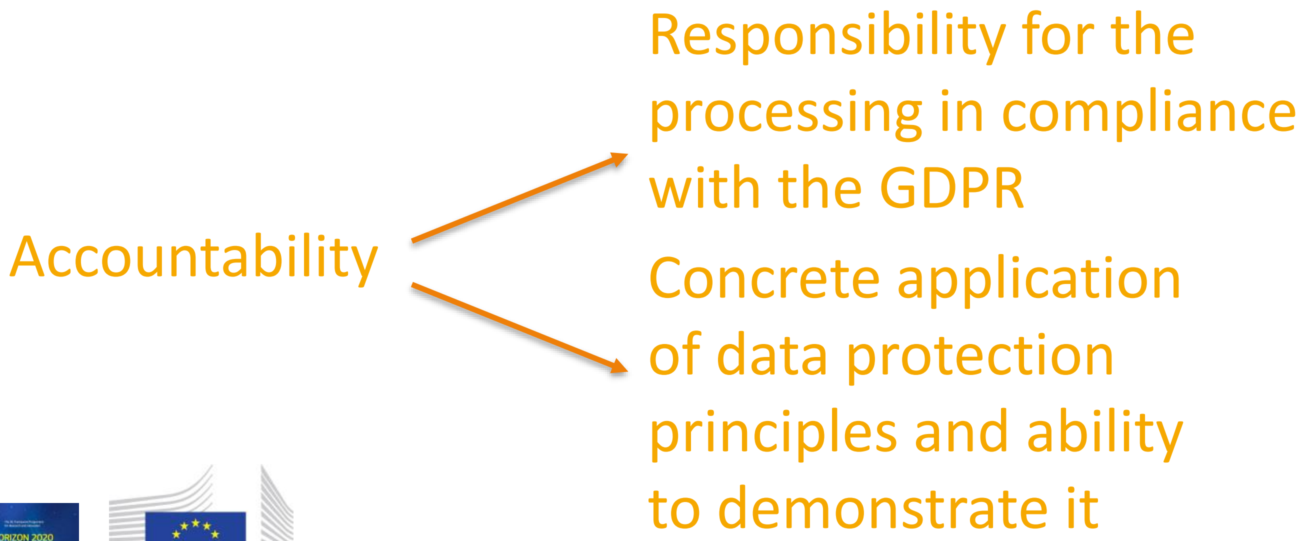
- Our guiding principles: ACCOUNTABILITY, TRANSPARENCY & SECURITY (Art. 5, GDPR) and **DP-by-Design/by-Default** (Art. 25, GDPR)

- Our goal: to define a **Data Protection Compliance Model** for the Consortium and the Project Tools management

Why a Model? To be accountable

- Art. 5.2 GDPR

The controller shall be responsible for, and be able to demonstrate compliance with all the principles of Art. 5.1



Accountability

Responsibility for the processing in compliance with the GDPR

Concrete application of data protection principles and ability to demonstrate it

Tasks of the Data Protection Office

- The DP Office is defining a ”**Data Protection Compliance Model”** for Privacy Flag, identifying the carried out data processing activities and providing guidelines and documents to comply with the General Data Protection Regulation requirements related to the Project

- The method of work: 4 steps to be taken from a Data Protection by Default/by Design perspective

HORIZON 2020

Steps of alignment to GDPR: Step 1 – MAPPING – DUE DILIGENCE & GAP ANALYSIS

- Data Protection requirements identification (Task 1.1 of the Project)

- Identification of data processing activities concretely actually, likely or potentially carried out by the Consortium today and in the future:
  - how personal data is processed and for what purposes
  - types of data
  - entities involved in the processing activities
  - data flow
  - period of storage of data
  - possible transfers of data to third countries

Steps of alignment to GDPR: Step 2 – FIRST LEVEL POLICY, CLAUSES AND PROCEDURES

- Adoption of the first documents in compliance with GDPR
  - Internal **roles** and data management **governance** scheme
  - Drafting **privacy policy and information** to data subjects
  - Drafting **Data Processing Agreements** (Art. 28, GDPR)
  - Appointment of a **Data Protection Officer** (Article 37, GDPR)
  - Designation of the natural persons authorised to data processing activities (Art. 29, GDPR)
  - Setting **procedures for the exercise of the rights** of the data subject (Article 12.2, GDPR)

Steps of alignment to GDPR: Step 3 – SECURITY AND RECORDS DESIGN/IMPLEMENTATION

- Definition of other essential elements in compliance with GDPR
  - Drafting of **Record of processing activities** carried out (Art. 30, GDPR)
  - By Design identification and implementation of the **security measures** with the technical partners for each PF Tool (Artt. 25, 32, GDPR)
  - Carrying out **Data Protection Impact Assessments** when needed
  - Provision of a **data breach procedure** and adoption of organizational measures adequate to the existing risk (Art. 32, GDPR)
  - Provision of a **data retention policy** (Art. 5.1.e and 25.2, GDPR)

Data protection requirements by design: only a few examples for the project architecture

Security of data storage

Anonymization

Information to the data subject

Purpose limitation

Limit minors of age participation

Data minimization

Consent withdrawal

Data breach information

Unambiguous consent

Right of access

Appropriate retention period

The aim is to include privacy-DP-legal aspects in the "DNA" of the project and of its tools: lawyers work with ICT engineers/experts and project coordinators, step by step

Steps of alignment to GDPR: Step 4 - CONTINUITY

- Giving continuity to the **Data Protection Compliance Model**:
  - ❖ Provision of a **process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures** for ensuring the security of the processing (Art. 32.1.d), GDPR)
  - ❖ Management, with the technical partners, of the **back-up and continuity of data systems** in the event of a physical or technical incident (Article 32.1.c), GDPR)

Main challenge: monitoring of fulfillment of PF data protection requirements

Thank you for your attention!

Luca Bolognini

PRIVACY FLAG

velti

DUNAV NET

Archimede Solutions SARL

University of BRISTOL

Istituto Italiano per la Privacy e la Valorizzazione dei Dati

National and Kapodistrian University of Athens

uni.lu UNIVERSITÉ DU LUXEMBOURG

CTI "DIOPHANTUS" computer technology institute & press

OTE

MANDAT INTERNATIONAL

HWCommunications Cyber Security and Resilience

LULEÅ UNIVERSITY OF TECHNOLOGY

MY DATA

PRIVACY FLAG

HORIZON 2020