PRIVACY & SECURITY

Second International TRUSTaWARE meeting

ABI Lab Forum - 27 March 2024

Romano Stasi

General Secretary, ABI Lab

The TRUSTaWARE Project

ABI Lab

TRUST aWARE

BACKGROUND

TRUST aWARE's mission is to provide a holistic and effective digital Security & Privacy (S&P) framework comprising a set of novel and integrated tools and services co-created by citizens and stakeholders.

This framework will help to identify, audit, analyse, prevent, and mitigate the impact of the various S&P threats associated with citizen's digital activities in a timely manner, while enhancing software trust and regulatory compliance.

The main TRUST aWARE results that will be presented later by the Project Partners

This project has received funding from the European's Union Horizon 2020 research and innovation programme under Grant Agreement n. 101021377.

Second International TRUSTaWARE meeting Agenda

Welcome speech
Romano Stasi, *General Manager* **ABI Lab**

Guido Scorza, **Garante per la protezione dei dati personali**

Ifigeneia Lella, **ENISA**

TRUST aWARE Technical partners – Tools presentation:
Chair: Javier Gutierrez Meana, *R&D Manager* **Treelogic**, *Project Leader* **TRUST aWARE**

- Privacy Adviser
  Cristian Robledo, **Treelogic**
- MISP Guide Demo & Taxonomy
  Gabriele Gamberi, **CERTFin**
- TRUST aWARE dashboard
  Andrés del Álamo, **Fundación Cibervoluntarios**
- The Dashboard Demo
  Pavlos Katsifarakis, **Trilateral Research**
- Static Analysis
  Gabriel Hortea, **UC3M**
- Dinamic Analysis
  Aniketh Girish, **IMDEA**
- CheckMyNews
  Salim Chouaki, **CNRS**
- The Activity Monitor
  Broderick Aquilino, **With Secure**

Closing remarks
Emiliano Anzellotti, **ABI Lab**
Rigo Van den Broeck, *Executive Vice President Cyber Security Product Innovation* **Mastercard**
Paweł Pawliński, **CERT PL**

Key challenges for financial sector

ABI Lab

Encourage the adoption of innovative technologies in banking and financial operations while striking a balance between leveraging service advancements and upholding individuals' rights to "privacy“

Facilitate a data exchange ecosystem (Open Data) that complies with privacy regulations and streamlines secure data transfer processes

Enhance alignment between the regulations governing the banking/financial sector at both national and European levels, and the legislation concerning data processing

Promotion of new technologies

ABI Lab

BACKGROUND

- **Big data, data analytics, machine learning** have gained significant traction in the banking and financial sector, drawing substantial investments.
- In Italy, **the banking sector has initiated discussions to pinpoint solutions that align with various regulations** like the IA Act, GDPR, among others. Assurance mechanisms are being considered to uphold the rights and freedoms of all involved parties.
- It is possible to use **systems of analytics or Artificial Intelligence to «anticipate» or adequately manage** the risks that characterize the banking system (e.g. credit risks).

CHALLENGES

Encourage the adoption of innovative technologies in banking and financial operations while striking a balance between leveraging service advancements and upholding individuals' rights to "privacy"

- **The drive for innovation pushes banks toward becoming more data-driven, presenting new compliance challenges related to Analytics, AI, and Big Data**
- **New technologies require continuous reassessment of data and information**
- **Incorporating innovative tools should prioritize data minimization and establish clear accountability for the Data Controller, especially in automated procedures and analyses**
- **Transparency of algorithms**

ACTIONS

- Initiate **proactive measures to facilitate ongoing dialogue between the banking sector, Fintech, and Supervisory Authorities** in privacy and banking oversight. This fosters a deeper understanding of banking complexities and the advantages of appropriately balanced use of innovative technologies, safeguarding customer privacy.
- Create **new skills to understand and manage the complexity of new technologies** and their speed of evolution in a data-protection perspective and strengthen customer awareness.
- **Enhance collaboration and communication among data controllers and all stakeholders involved in data management processes**.

Data transfer and exploitation of Open Data

ABI Lab

BACKGROUND

- The issue of **the transfer of personal data in non-EU countries** is hugely critical, especially after the decision of the European Court of Justice cd. Schremes II and the Provision so-called "caffeine" on Google Analytics.
- It is difficult to rely on **a valid tool that can be provided as evidence of accountability** for managing risks associated with data transfer activities to some non-EEA countries.
- **Greater exploitation of Open Data could facilitate data transfer procedures in third countries**, between companies of the same banking/financial group while maintaining an adequate degree of security.

CHALLENGES

Facilitate a data exchange ecosystem (Open Data) that complies with privacy regulations and streamlines secure data transfer processes

- **Extra EU data transfer**
- **Data transfer to Third Parties (broad eco-financial system)**
- **Data transfer within the same corporate group**
- **Data transfer and sharing to enhance the security of financial services**

ACTIONS

- Establish a **regulatory framework equipped with practical tools aiding controllers in performing TIAs** (Transfer Impact Assessments). This initiative aims to offer unified guidance and certainty regarding the robustness and legal validity of transfer mechanisms. Simultaneously, it **supports the advancement of Open Data**, particularly within the banking and financial sectors.
- **Enhance opportunities for sharing personal data within cybersecurity and anti-fraud domains to bolster customer protection.**

Coordination between GDPR and industry regulations

ABI Lab

BACKGROUND

- **The legislation on the processing of personal data has a horizontal scope.** This characteristic has been subject to reconciliation with other regulations that provide specific provisions regarding the legitimacy or otherwise of the processing of personal data.
- A practical example is the interaction between the AML and the Privacy **(«right of access» and limitation, legal bases for processing for AML purposes, retention times).**
- **Information sharing (cybersecurity, AML etc.) between financial institution and Authorities is an added value that needs to be widely addressed at the regulatory level. The issue of balancing the rights of data subjects and the objectives of combating crime remains relevant.**
- **As part of the interaction between GDPR and the next PSR/PSD3 Directive, some topics remain in the center of the debate, (permissions/consent, processing of special category of personal data, dashboard to manage permissions, etc.).**

CHALLENGES

Enhance alignment between the regulations governing the banking/financial sector at both national and European levels, and the legislation concerning data processing

- **Right of access to data, deletion of data, AML**
- **Evolution of digital identity management (PSD3, PSR, GDPR and eIDAS)**
- **Consistency between the different regulations currently under review**
- **Establish a fitting legal base for activities involving the infosharing**

ACTIONS

- **Ensure a greater coordination between the disciplines and a constant dialogue with the National Authorities to illustrate the specificity** of some disciplines with respect to the GDPR and report, in the European context, the need for greater "consistency" of the rules.
- **Identify a solid legal base for infosharing activities and perform – ex ante and with all the sectorial Authorities - a balance between the protection of data subjects and the public interest.**