



EUROPEAN DATA PROTECTION BOARD

Subject EU PAPAYA Project's Comments for EDBP Recommendations

Sophia-Antipolis, December 14th 2020

To Whom It May Concern:

To illustrate technical measures which provide high level of protection required under EU law in the context of a transfer of personal data to a third country, we can propose a use case in details in deliverable D2.1 of the Project (<https://www.papaya-project.eu/deliverables>) with advanced privacy enhancing technologies for data analytics.

The H2020 PAPAYA (Platform for PrivAcY preserving data Analytics) Project aims at addressing privacy concerns when data analytics tasks are performed by untrusted third-party data processors. In PAPAYA, these tasks can be performed obliviously on protected data (i.e. encrypted data) through the development of dedicated privacy preserving data analytics modules. These modules will enable data owners to extract valuable information from this protected data, while being cost-effective and accurate. The platform makes use of advanced privacy enhancing technologies such as homomorphic encryption, secure two-party computation, differential privacy and/or functional encryption to design and develop big data analytics operations. Data analytics operations range from simple statistics such as counting to more sophisticated machine learning techniques such as neural networks. Each module in the PAPAYA platform corresponds to a particular operation. The framework also offers end users the ease to control the use of their data and to exercise their data subjects' rights through the data subject toolbox. The data subject toolbox is used by the user of the platform in their data subject facing applications-such as mobile apps-to provide functionality that enable data subjects to assess risks and exercise control over their personal data. The overall architecture of the PAPAYA framework and its main components are described in details in deliverables D4.1 and D4.2 of the project (<https://www.papaya-project.eu/deliverables>). The framework also offers end users the ease to control the use of their data and to exercise their data subjects' rights through the data subject toolbox. The data subject toolbox is used by the user of the platform in their data subject facing applications-such as mobile apps-to provide functionality that enable data subjects to assess risks and exercise control over their personal data. The overall architecture of the PAPAYA framework and its main components are

described in details in deliverable D4.1 of the project (<https://www.papaya-project.eu/deliverables>).

Hence, data processing can be possible without revealing data to the platform in the third country. PAPAAYA modules could represent effective technical measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.

Yours faithfully,
EU PAPAAYA consortium
papaya@eurecom.fr