Rome, 30th of November 2020

To the kind attention of

European Data Protection Board

Rue Montoyer 30, B-1000 Brussels

InfoCert contribution to the open consultation on the "*Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*".

Dear European Data Protection Board,

It is a pleasure for InfoCert to contribute with some comments and considerations to the "*Recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data*", adopted by EDPB on 10th November 2020.

InfoCert is the leading European Qualified Trust Service Providers (QTSPs), operating in more than 20 countries in Europe and LATAM and offering a full service of digital services that add trust in digital transactions. We provide to our customers Qualified Certificates for Signature, Seal and Webserver Authentication and the services related to it, we are an Identity Provider entitled by the Italian Government to provide the national digital identity (SPID) and a Local Operating Unit accredited by GLEIF to issue Legal Entity Identifiers and we manage billions of transactions with our customer onboarding, delivery and document archiving services. In addition, we are active in the field of blockchain-based Self-Sovereign Identity and Identity of Things and we continuously explore new innovative solutions, thanks to our innovation lab.

Your Recommendation on data transfer points out several relevant tools to fulfil the obligation set out in the General Data Protection Regulation, and we noticed that it often underlines the importance of encryption to protect personal data during the transfer and the storage. Encryption is in the DNA of a QTSP: the generation and management of cryptographic keys is the main element behind a Qualified Signature, a Qualified Delivery Service, Qualified Certificates in general, but even in Digital Identity and Long-Term Document Preservation and Archiving. Beside encryption and technology, a QTSP always connects technology with a strong layer of compliance, thanks to audits, a vigilance scheme and a clear liability framework that empower the security and the value brought to the Digital Single Market.

In the aftermath of the EU Court of Justice recent judgment C-311/18 (Schrems II), and in a context where even more Data Controllers transfer European citizens' personal data to third Countries, we believe that QTSPs can represent an important safeguard for the right of subjects and data controllers, especially when dealing with cloud providers and servers located outside EU. Unfortunately, GDPR and the other data processing legislations and resolutions don't directly refer to the eIDAS Regulation and the role of trust providers, creating a lack of connection and interoperability between the two main pillars of the European regulation of digital transactions.

On this basis, we kindly propose you to consider in the Recommendation the use of eIDAS trusted services like qualified electronic seals (QSeals) and qualified website authentication certificates (QWACs), that can be paramount to reach two main objectives in the protection of transferred data: the confidentiality of archived data and the protection of data during its transit, adding in addition a clear traceability of the liabilities of the involved providers.

The confidentiality of stored data can be reached through **encryption**, that should be carried out before, during and after the transmission of data, so ensuring that the access to the data is only possible with the authorization of the Data Controller. The use of a **Qualified Certificate for electronic Seal** can ensure that the data transferred to a Data Importer (even located in a third country) remain intact, so that the transfer activity fully complies with the current data protection legislation. With a Qualified Certificate for Seal, encryption keys used to cipher data are generated by a QTSP only after a strict vetting process of the legal person that requests it, ensuring that the Data Controller can be the only entity with the possession of the means to decrypt the data, with the additional guarantee given by the QTSP that cryptographic keys are securely held, managed and used thanks to the use of a Qualified Signature Creation Device.

Moreover, in order to **secure the channels** through which the encrypted personal data are transmitted to the third country-located Data Importer, we propose the use of **Qualified Webserver Authentication Certificates** to secure the connection. By adopting it, the servers of Data Exporters and of Data Importers can be identified and connected to the legal person managing it, underlining and **tracing the roles** of the players involved in the liability schema designed by the GDPR and defining which are the providers with a gatekeeping function. This architecture based on Qualified Certificates for Seal and Web Authentication has already been experimented with a great success in another context: the communication between servers of financial institutions and Payment Providers in the context designed by the Directive (EU) 2015/2366 on payment services in the internal market (PSD2). When a Payment Provider or an Account Information Service Provider connects to the open banking services of a Bank, all the communication and the data transfers are secured using QWAC certificates as defined by the Regulatory Technical Standards issued by the European Banking Authority that choose eIDAS certificates as a way to give trust to the entire system.

We strongly believe that eIDAS trust services and Qualified Trust Service Providers can serve the purpose stated by the General Data Protection Regulation, effectively enforced by EDPB and the Privacy Authorities in every Member State.

InfoCert, as the leading European QTSP, remains available for the Board and the National Authorities to better define and deep our proposals, if needed, and for any further need.

To this end, you can contact the following email addresses:

- Igor Marcolongo (Innovation and Strategy – Head of Business Compliance): *igor.marcolongo@infocert.it*;
- Andrea Garilli (Innovation and Strategy – Digital Consultant): *andrea.garilli@infocert.it*.

We also would like to take this opportunity to send you our best regards.

InfoCert S.p.A.