EU Data Protection Regulators Publish Additional Guidance On The EU-U.S. Data Privacy Framework

August 19, 2024 By Wim Nauwelaerts

Last month, the European Data Protection Board – which is composed of the national data protection authorities ('Supervisory Authorities') of the countries in the European Economic Area ('EEA'), as well as the European Data Protection Supervisor ('EDPS') – adopted two Frequently Asked Questions ('FAQ') documents concerning the EU-U.S. Data Privacy Framework ('DPF'), aimed at providing further insight into the functioning of the DPF. The European Commission considers that transfers of personal data from the EEA to companies in the U.S. certified under the DPF enjoy an adequate level of protection. As a result, personal data can be transferred freely from the EEA to U.S. certified companies, without the need to put in place additional data transfer safeguards.

The first FAQ informs individuals about the DPF in general, how to benefit from it, how to lodge a complaint under the DPF, and how their complaint will be managed.

The second FAQ focuses on businesses that are considering DPF certification: it explains which companies are eligible to join the DPF, what to do before transferring personal data to a company in the U.S. that is DPF-certified, and where to find additional guidance.

Below is a summary of the Board's key recommendations for businesses:

1. The DPF applies to any type of personal data transferred from the EEA to the U.S., including personal data processed for commercial or health purposes, and human resources data collected in the context of an employment relationship, as long as the recipient company in the U.S. is self-certified under the DPF to process those types of data. This means that the DPF can also be used to transfer, for instance, clinical study-related data from patients in the EEA to U.S.-based study sponsors that have certified under the DPF.

2. Non-profit organizations, banks, insurance companies and telecommunication service providers which do not fall under the authority of the U.S. Federal Trade Commission ('FTC') or the U.S. Department of Transportation ('DoT') cannot self-certify under the DPF. In order to be eligible to self-certify to the DPF, a company in the U.S. must be subject to the investigatory and enforcement powers of the FTC or DoT. However, according to the Board, other U.S. statutory bodies may be included in the future.

3. Before transferring personal data to a company in the U.S. that claims to be self-certified under the DPF, the EEA-based data exporter must verify and confirm that the company in the U.S. holds an active self-certification to the DPF, and that this certification covers the transferred data.

4. The DPF List – published on the U.S. Department of Commerce's website – includes a register of companies that have been removed from the List ('inactive participants'). An EEA data exporter cannot rely on the DPF for transfers of personal data to such companies. The Board also emphasizes that companies that have been removed from the DPF List must continue to apply the DPF Principles to personal data received while participating in the DPF, for as long as they retain the data.

5. Self-certification under the DPF will enable data exporters in the EEA to comply with Chapter V of the GDPR (on transfers of personal data to third countries or international organizations), but all other requirements in the GDPR and national data protection law remain applicable, including:

    - When an EEA controller transfers personal data to a processor in the U.S. that has self-certified to the DPF, the controller and processor must enter into a data processing agreement that meets the requirements of Article 28 GDPR;

    - EEA data exporters can only share personal data with a company in the U.S. if there is a legal basis for the data sharing/transfer (in accordance with Article 6 of the GDPR). Also, prior to transferring personal data to a self-certified company in the U.S., data exporters in the EEA must ensure compliance with Articles 13 and 14 GDPR and inform individuals about the identity of the recipients of their data and about the fact that the transfer is covered by the DPF.

6. If personal data is transferred to companies in the U.S. that are subsidiaries of a DPF-certified parent company, the EEA-based data exporters must ascertain that the certification of the parent company also covers subsidiary companies.

Filed Under: Privacy Tagged With: GDPR

Wim Nauwelaerts is a partner in the Brussels office, leading Alston & Bird's European Privacy, Cyber & Data Strategy Team. Wim has over 20 years of experience working with global companies on their data protection, privacy, and cybersecurity needs, including General Data Protection Regulation (GDPR) readiness, data transfer, data security and breach requirements, and compliance training.