EDPB Releases Statement on the Processing of Personal Data in the Context of Reopening Borders Following the COVID-19 Outbreak

Monday, June 22, 2020

On June 16, 2020, the European Data Protection Board (the “EDPB”) released a statement on the processing of personal data in the context of reopening borders following the COVID-19 outbreak (the “Statement”).

Following the EU Commission’s decision to lift internal border controls, countries are implementing measures to control the flow of individuals entering into and/or travelling within their territory (such as COVID-19 testing, requiring a certificate issued by a health professional and using voluntary contact tracing apps) that involve the processing of personal data. In its Statement, the EDPB states that such measures cannot affect individuals’ fundamental rights and freedoms, particularly the right to data protection. In light of this, the EDPB urges EU Member States to take a common approach when deciding which processing activities are necessary to stop the spread of the virus while ensuring respect for fundamental rights and freedoms of individuals. The EDPB also emphasizes that processing activities taking place in this context should meet the necessity and proportionality tests and should be based on scientific evidence.

The Statement also lists aspects of the EU General Data Protection Regulation (“GDPR”) that require Member States’ special attention:
Lawfulness, fairness and transparency: The processing must be fair and transparent towards the data subject and satisfy one of the legal bases offered by the GDPR.

Purpose limitation: Purposes should be specified for the data subjects and the processing should be limited to the purpose of fighting the spread of the virus and facilitating the provision of necessary health care.

Data minimization: Member States should only process data that is adequate, accurate, relevant and limited to what is necessary to achieve the purpose for which it is processed.

Storage limitation: Data should only be kept for a short period and no longer than necessary for the processing purpose.

Security: Member States should ensure the appropriate level of security by implementing technical and organizational measures based on risk assessments.

Data protection by design and by default and data protection impact assessments: Member States should ensure data protection by design and by default and, where applicable, conduct data protection impact assessments.

Data sharing: Data processing agreements should be in place when personal data is shared with processors and the parties’ responsibilities should be clearly defined, including when sharing personal data with public authorities.

Automated decision making: The decision to allow entrance into a country should not only be based on the available technology but also should be subject to suitable safeguards.

Finally, the EDPB stresses the importance of a prior consultation with competent data protection authorities (“DPA”) when Member States process personal data in this context, in order to facilitate the correct application of the GDPR. As an example, the Belgian DPA recently announced that it has, on its own initiative, contacted Brussels Airport to better understand the temperature check technology the airport is using and the legal basis relied on to legitimize such controls.

Copyright © 2020, Hunton Andrews Kurth LLP. All Rights Reserved.

National Law Review, Volume X, Number 174