Data protection: rights of passengers using Automated Border Control

As news emerges that the European Commission's counter-terror plan will require blanket collection and storage of personal data records of all passengers flying in and out of Europe, ***Diana Dimitrova from KU Leuven*** *returns to discuss rights of passengers using Automated Border Control. The passenger rights discussed here have broader implications for all data subject to the Data Retention Directive.*

In a previous blog post I discussed certain legal aspects applicable to Automated Border Control (ABC). I argued that ABC changes the nature of identity verification at the external borders of the European Union as it introduces biometrics as a "token" for *automated* identity verification. *Automated biometric verification* is currently not a requirement under the Schengen Borders Code as concerns EU/EEA/CH passengers, however. As to Third Country Nationals (TCNs) who are visa holders, there *is indeed* an obligation to compare their fingerprints against the fingerprints stored in the VIS (Article 18 VIS Regulation).

Storage of data

One of the novelties of the automated biometric verification is that it provides the opportunity to store passenger data processed at e-Gates/kiosks. One way is through the establishment of a Registered Traveller Programme (RTP), whereby a database is created for a certain period of time for passengers who voluntarily enroll and the data, including biometrics, is supposed to be deleted when the registration expires.

In other cases, however, the storage might not be so obvious. For example, the alphanumeric data from the passport, the biometric data from the chip of the passport and the live biometric images captured at the kiosk/e-Gate could, technically speaking, be stored after the passenger has crossed the border.

Thus, I recommended the immediate deletion of the data at the end of the process. The recommendation responds to the following concerns:

- ABC is designed to process data for border control purposes, which is regulated by the Schengen Borders Code (SBC) and applies to all current and prospective Schengen States. For EU/EEA/CH travelers, personal data are needed to verify that the passenger is the rightful holder of the travel document, the latter is not lost/stolen/misappropriated and invalidated (search in SIS II and national databases), and on a non-systematic basis that the person is not a wanted person. More entry requirements apply to TCNs, one of which is the verification of fingerprints for visa holders (see Art. 7 (2) and (3) SBC). None of the requirements of the SBC relate to storage of personal data (e.g. biometrics of EU/EEA/CH citizens) at external borders. Once the border check is carried out, the data are not further needed. Sometimes certain data could be stored, though, if the national law provides for a national Entry – Exit System, but it usually applies to TCNs.
- Talking about border control purposes, let us be reminded that one of the cornerstone principles of data protection is purpose limitation, i.e. processing of data only for a specified purpose, e.g. border control. Data may not be processed for other, incompatible aims. The data, thus, should not be stored longer than necessary for the purpose of checking persons at the border. The issue with storing data after the completion of the border control process is that it makes it available for further re-use, such as for law-enforcement purposes. The latter is an incompatible purpose as crossing borders is not an illegal act *per se.* Indeed, databases on lost and stolen objects (e.g. passports) are checked systematically for all passengers and checks on persons in databases (e.g. criminals) are checked non-systematically in the case of EU/EEA/CH and systematically as concerns TCNs. However, storing (biometric) data of all passengers, who are presumably innocent, and potentially interlinking and cross-matching them with law-enforcement databases, risks placing everyone under general suspicion and would be incompatible

with the original purpose. Following the ruling on the Data Retention Directive, storing data on individuals for law-enforcement purposes when there is no link, even indirect, between the person and serious crime, would be illegal.

How does the storage of data affect your rights as users of ABC?

Right to information

In the first place, you have the right to be informed what data the particular ABC installation processes on you and how it processes your data: would it store any data, who will have access to it, etc? To whom should you turn to request information or complain, i.e. who the controller of the data is? What other rights as data subjects do you have? To provide this information is a requirement for the controller and to have it is a basic right of the passenger.

Right to access

You have the right to inquire whether information is stored on you and to access this data. If you use the e-Gates and would like to know whether any of your data was stored, you must be given access to this information, as well as to a copy of the data on you. This right could be restricted only in limited cases such as criminal investigations and prosecutions (Article 13 Directive 95/46/EC) subject to national law. However, it would not be justified to treat all passengers as suspects as that would contradict the presumption of innocence.

Right to rectification, erasure and blocking

If you learn that data are stored on you, also outside the framework of an RTP, you may request their deletion or blocking if the storage is contrary to the law. You can also wish to have the data corrected in case it is not accurate.

Right to object

Currently under EU law there is no obligation to use ABC technology. Therefore, you have a choice whether to use it or not. Thus, you may object at any time to using ABC kiosks and e-Gates.

Right to submit a complaint and to remedy

If you believe that your rights have been infringed, you must always be given the opportunity to submit a complaint to the controller and also to the relevant national data protection authority to remedy the infringement under the procedures of the applicable national law.

The deployment of ABC entails certain data protection limitations and obligations for the authorities that operate them. The effective exercise of the rights of the data subjects (ABC users) is one way to enforce these obligations and avoid potential abuse.

This article gives the views of the author, and does not represent the position of the LSE Media Policy Project blog, nor of the London School of Economics and Political Science

---

January 28th, 2015 | Featured, Privacy | 1 Comment
