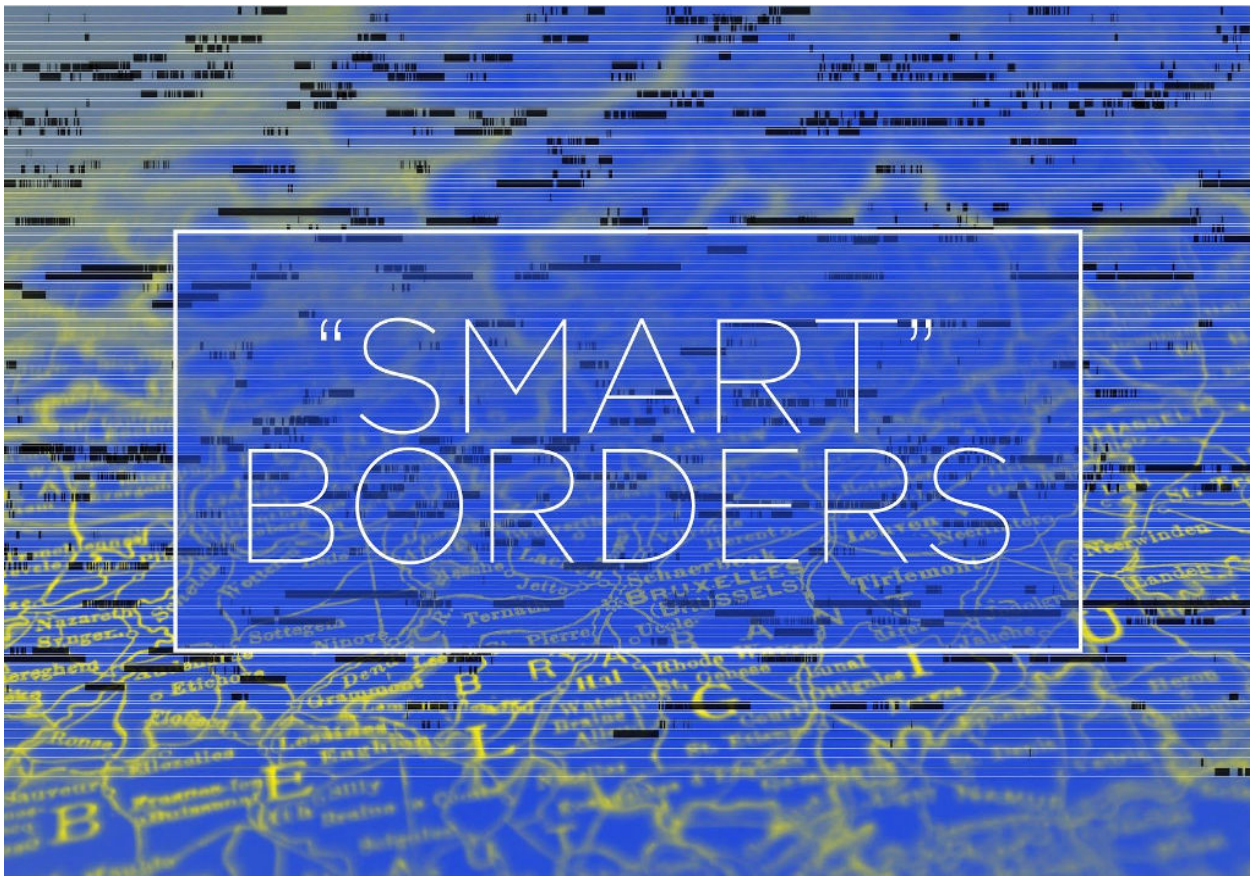
accessnow

# Smart Borders Policy Analysis




## Executive Summary

The following paper provides an analysis of the impact of the EU Commission's "2016 Smart Borders package" on the fundamental rights to privacy and data protection protected by Article 7 and 8 of the EU Charter. The paper is divided in two sections: border management purposes and law enforcement purposes. The analysis is based on the jurisprudence of the EU Court of Justice as well as opinions and studies from the EU Fundamental Rights Agency, the EU Commission Impact Assessment, the Article 29 Working Party, the European Data Protection Supervisor, Europol, EU-LISA, and the EU Committee of the Regions. The analysis finds that despite efforts of the EU Commission to consider the protection of the fundamental rights to privacy and data protection, the troubling issues in the 2013 draft of the package have been exacerbated. The latest proposal has added a new purpose for access and use of data by law enforcement authorities that is not sufficiently justified; would create a massive database of sensitive information; lacks a comprehensive oversight mechanism; provides insufficient access to redress mechanisms; has loose rules for access and transfer of data; and includes disproportionate data retention mandates.

## Table of contents

## Introduction

Access Now (accessnow.org) is an international organisation that defends and extends the digital rights of users at risk around the world. We are a team of 40, with local staff in 10 locations around the world. We maintain four legally incorporated entities — Belgium, Costa Rica, Tunisia, and the United States — with our tech, advocacy, policy, granting, and operations teams distributed across all regions. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.

We defend privacy globally. Access Now provided comments on the development and implementation of data protection and privacy rules in the Brazilian Marco Civil, the African Union Convention on Cyber Security and Personal Data Protection, and the US Federal Communications Commission's broadband privacy rules. In the EU, we have been involved in the EU data protection reform process since the tabling of the General Data Protection Regulation (GDPR) by the EU Commission in January 2012. We developed a policy paper in the review of the e-Privacy Directive; and commented on the Privacy Shield, Umbrella Agreement, and Passenger Name Records proposals. Specific to the review of the Smart Borders package, we provided input to the Commission's public consultation.

In this paper, Access Now provides an analysis of the impact on the fundamental rights to data protection and privacy of the EU Commission's 2016 revised proposal on the Smart Borders package, with a particular focus on the proposal for a Regulation establishing an Entry/Exit System (EES). The 2016 Smart Borders proposal differs from the original 2013 draft, as it:

- includes a new purpose for law enforcement access and use of traveller data gathered during border controls. The original proposal had a single purpose: to improve border management for travellers entering the EU, with the objective of reducing waiting time at border checks, improving the quality of identity checks, and gathering more accurate information on so-called overstayers.
- extends the data retention period from 181 days to 5 years; and
- merges the proposal for the creation of a Registered Traveller Programme (RTP) into the EES.

In this analysis, we first examine the proposed measures for collection, storage, and access to data for border management purposes, then address the newly proposed use of the instrument for law enforcement purposes.

## 1. Use of Data for Border Management Purposes

### *a. Overly broad collection of biometric data*

The revised proposal for establishing an Entry/Exit system foresees the collection of biometric data from third-country travellers who do not have EU residence permit: four fingerprints and a facial image. Notably, the 2016 EU Commission impact assessment indicated that the law **should not allow collecting biometric data from people under 18 years old**, as reflected in the results of the study conducted by the EU Fundamental Rights Agency (FRA) during the Smart Borders pilot. Yet a provision to disallow such collection is not included in the proposal for an EES. The same FRA study also showed that one fifth of people participating in the pilot project found collection of biometric data, including fingerprints, to be **intrusive and humiliating**.

The proposal also foresees vast data collection. According to the impact assessment, the collection and storage of biometric data is expected to concern 76 millions travellers per year starting in 2025. These data will be retained for five years and merged with data available in the Visa Information System (VIS), creating the **largest database of sensitive data in the European Union**. Surprisingly, the Commission in its impact assessment considers the existence of a single database an example of privacy by design. Yet creating a single giant database opens up significant risks for the fundamental rights to privacy and data protection, due to the amount of data stored, the risk of unauthorised access to the data, and the lack of robust data protection safeguards in the proposal. A true implementation of the privacy-by-design principle would require limiting data collection, limits to how long it is stored, and strict rules for access to data and keeping it secure.

**Recommendations:**

- **Limit the collection of biometric data, and**
- **Promote privacy-by-design tools, such as data shredding or encrypted storage, rather than establishing a massive database of sensitive information.**

### *b. Deficient rules for access to personal data and remedy*

The EES and relevant impact assessments highlight the importance of ensuring limited and justified access to stored data. The measures put forward, however, fall short of achieving this aim. The proposal **lacks measures to guarantee the security and integrity of the data stored**. Experience from the Data Retention Directive shows that authorities and third parties can abuse massive databases. It is no secret that a massive database of biometric information would be of high value both to **intelligence agencies around the world** and the **surveillance industry**. It is of the utmost importance to ensure that the creation and maintenance of databases is not handed over to companies that are part of mass surveillance schemes or have been compromised by intelligence agencies.

Lastly, the proposal lacks safeguards to ensure efficent oversight and access to remedy. Specifically, to ensure right to remedy for travellers, it is crucial that travellers have information available in their languages on their data protection rights (access, rectification and more), as

well as information about how and where to lodge a complaint, and access to legal assistance and translation services, if necessary.

**Recommendations:**

- **Allocate contracts for building EES to companies providing systems that guarantee high standards for security, recognised by independent parties, and that promote resilience to surveillance,**
- **Inform users about their rights, and**
- **Provide travellers with access to legal assistance and translation services.**

### *c. Unclear added value of proposal*

The EES foresees first collecting biometric data to create a file for each traveller and then subsequently using either a fingerprint or facial image for re-identification at every border crossing. It is unclear how the complex process foreseen would lead to more efficient or reliable border controls. The Committee of the Regions opinion in 2013 found that collecting biometric data would **increase traveller waiting time at the borders check**, a point partially acknowledged in the EU Commission impact assessment. In practice, collecting biometric data is not always feasible. It is important to note that adverse climate conditions can make fingerprint collection and checking at some borders impossible, as pointed out by border guards. Furthermore, the Article 29 Data Protection Working Party (WP29) indicated that such a time-consuming process "entails a risk of error" and that "creating a large scale database holding biometric data in order to streamline procedures at border crossings, is **not proportional**".

The added value of establishing an EES for border management is unclear, since the new proposed system would only increase the waiting time at borders. Furthermore, the EU Commission failed to demonstrate the necessity and proportionality of most of the measures, thus putting the legality of the proposal into question. The proposal could perhaps lead to the production of better and more accurate statistics for eu-LISA and Fontex, but the risks to fundamental rights it raises, and its heavy financial costs for member states, outweigh these limited benefits.

**Recommendations:**

- **Conduct necessity and proportionality test of the proposed measures in relation to the border management purpose.**

## 2. Use of Data for Law Enforcement Purposes

### *a. Unjustified purpose*

The most notable modification from the 2013 to the 2016 EES proposal is the **unjustified** addition of a new purpose, which would enable law enforcement authorities (LEA) to access and use the data collected at the border. While the Commission's impact assessment considers access by LEA potentially "useful" — but not necessary — the European Data

Protection Supervisor (EDPS) considers the measure "not sufficiently supported by convincing evidence". Furthermore, several EU information systems, including Eurodac, VIS, and the Schengen Information System II (SIS II) already grant LEA access to information on third-country nationals entering the EU. Does the Commission seek to grant LEA access to EES because VIS, Eurodac, and SIS II are not functioning? Limited information is available on the functioning and efficiency of those existing databases. **Detailed assessment of existing systems must be conducted** before considering building a new system and comprehensive **necessity and proportionality tests must be conducted** before granting LEA access.

As a reference, in March 2012, the French Constitutional Council found a law proposing a new biometric identity card for French citizens unconstitutional and objected to the creation of a massive database that could be accessed and used by law enforcement authorities for a wide range of purposes, from identifying the victims of accidents to finding the perpetrators of infringements and crimes.

**Recommendations:**

- **Remove all articles and recitals related to the new and unjustified law enforcement purpose, unless the Commission is able to demonstrate the necessity and proportionality of the measures.**

*b. Excessive retention of data*

The extension of the data retention period from 181 days to 5 years is one of the most significant changes from the 2013 original proposal. A **data retention mandate** of five years for both border management and law enforcement purposes is **unjustified, excessive, and disproportionate**. The proposal also **fails to provide the necessary safeguards developed by the jurisprudence of the EU Court of Justice** in the Joined cases C-293/12 and C-594/12.

The Commission's impact assessment and proposal indicate that this retention period would be "useful" for LEA and "appropriate". Those legally untested standards cannot replace the necessity and proportionality tests that must be conducted when introducing a measure that constitutes a limitation of the right to privacy and data protection. In the absence of those tests, the WP 29 and the EDPS expressed serious doubts regarding the lawfulness of this proposal.

In short, the data retention mandate proposed by the Commission is **unjustified**, **fails to comply with the standards established by the CJEU**, would have a **deleterious impact on human rights,** and represents **high financial costs**.

**Recommendations:**

- **Conduct necessity and proportionality test and verify compliance of the data retention provision with CJEU case law.**

*c. Disproportionate access to and transfer of information*

Access to data collected for the EES by law enforcement authorities, including EUROPOL, creates obvious risks for the fundamental rights to privacy and data protection. The vagueness of the provisions and flexibility left to member states and national authorities to define rules on data access could lead to fragmentation, unequal protection, and potential misuse or abuse of data.

In addition, data could be shared not only with authorities in the EU but also **with third countries, international organisations, or private parties pursuant to the broad exceptions** in Article 38. Sensitive data could therefore end up in the hands of countries, authorities, institutions, or companies with insufficient and inadequate standards for privacy and data protection. It is unclear how this **extremely disproportionate measure** would be compliant with EU law and the jurisprudence of the Court developed in the case C-362/14.

**Recommendations:**

- **Remove all articles and recitals that allow data sharing with EU law enforcement authorities and third countries.**

## Conclusion & recommendations

We acknowledge the efforts of the EU Commission to consider the protection of the fundamental rights to privacy and data protection in the revised 2016 Smart Borders package. Unfortunately, the issues in the 2013 draft proposal are now exacerbated by the unjustified new law enforcement purpose; the creation of a massive database of sensitive information; flawed rules for oversight, remedy, and access and transfer of data; and disproportionate data retention. Furthermore, the cost of the proposal — which has been transferred to Member State budgets — remains extremely high, especially given its poor added value.

Access Now urges the European Parliament to significantly amend the Commission proposal to restore robust protection for fundamental rights and bring the proposal in line with EU law. Specifically:

- **All articles and recitals related to the new unjustified law enforcement purpose should be removed,** as the measures are neither necessary nor proportionate, and the proposal creates significant risks for privacy and data protection.
- **The collection of biometric data should be limited, and rules on storage should promote tools for privacy by design,** such as data shredding or encrypted storage, rather than merging and establishing a single massive database of sensitive information.
- **Travellers should have access to legal assistance and translation services.**
- Furthermore, we **invite the Civil Liberties Committee of the EU Parliament to organise hearings and seek legal advice** on the risks this proposal creates in relation to intelligence authorities and surveillance by private parties, in order to develop robust safeguards.
- Contracts for building EES should be conferred **only to companies providing systems that guarantee high standards for security, as assessed by independent parties,** and which promote resilience to surveillance.
- Lastly, adoption of the proposal must be contingent upon the **presentation of evidence from the Commission on the necessity and proportionality** of the proposed measures and an assessment of the existing EU information systems.

**For More Information**
Please visit www.accessnow.org

**Contact**
Estelle Massé | Senior Policy Analyst | estelle@accessnow.org

## References


- Article 29 Working Party, 2013. *Opinion on Smart Borders* http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf
- Conseil Constitutionnel, 2012. *Décision n° 2012-652 DC du 22 mars 2012 sur la loi relative à la protection de l'identité* http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2012/2012-652-dc/decision-n-2012-652-dc-du-22-mars-2012.105165.html
- Committee of the Regions, 2014. *Opinion on 'Smart Borders package'* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013AR3534&from=EN
- Court of Justice of the European Union, 2014. *Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Ireland and the Attorney General, and Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl and Others (C-594/12) - Joined Cases C 293/12 and C 594/12* http://curia.europa.eu/juris/document/document.jsf?text=&docid=153045&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=778015
- Court of Justice of the European Union, 2015. *Maximillian Schrems v Data Protection Commissioner Case C-362/14* http://curia.europa.eu/juris/document/document.jsf?text=&docid=172254&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=775541
- European Commission, 2016. *Impact Assessment Report on the establishment of an EU Entry Exit System* http://eur-lex.europa.eu/resource.html?uri=cellar:5c20aef7-fca4-11e5-b713-01aa75ed71a1.0001.02/DOC_2&format=PDF
- European Commission, 2016. *Regulation for the establishment of an Entry/Exit System (EES)* http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/regulation_proposal_entryexit_system_borders_package_en.pdf
- European Data Protection Supervisor, 2016. *Opinion on the Second EU Smart Borders Package* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-09-21_Smart_Borders_EN.pdf
- EUROPOL, 2012. *Data protection at EUROPOL.* Luxembourg: Publications office of the European Union.
- eu-LISA, 2015. *Smart Borders Pilot Project Report on the technical conclusions of the Pilot* http://www.eulisa.europa.eu/Publications/Reports/Smart%20Borders%20-%20Technical%20Report.pdf
- Fundamental Rights Agency, 2015. *Do travellers to the EU trust fingerprinting?* http://fra.europa.eu/en/news/2015/do-travellers-eu-trust-fingerprinting