7 Border management law in the European Union

Alessandra Calvi
Vrije Universiteit Brussel. E-mail: alessandra.calvi@vub.be.

7.1 Introduction

7.1.1 The concept of border management

The twofold goal of border management is to facilitate the efficient flow of *bona fide* travellers while preventing the entry of irregular travellers.[1] Traditionally, border management encompasses an ensemble of activities aimed at controlling the flow of goods and individuals across borders, and administering immigration, migrant flows and asylum requests. At the European Union level, instead, the focus of the so called "integrated border management" is rather on persons than on goods. Integrated border management is considered a necessary corollary to the free movement of persons and central to improve migration management (see *infra*). Its aims include efficiently managing the crossing of the external borders and addressing migratory challenges and potential future threats at those borders, while fully respecting fundamental rights.[2] In recent decades, the way in which border management in the European Union (EU) and in other Western democratic countries in general has been practiced has undergone significant changes, becoming increasingly technologised and digitalised. Traditional physical borders have been supplemented by new digital borders in the form of large-scale information systems that target primarily the movements of third-country nationals,[3] weakening the role played by the physical aspect of border management, including the actual crossing of territorial borders.[4] New border control technologies, which have become increasingly reliant on systematic and large-scale processing of personal data, especially biometric data, have been deployed with the objective of enhancing the efficiency of mobility control and increasing security.[5] Checks at territorial borders have become progressively automated and combined with checks before and during travel, as well as after arrival, now commonly in place.

DOI: 10.46944/9789461171375.7

At the same time, geographical frontiers are increasingly surveilled in order to prevent their crossing by irregular migrants.[6] Technological experiments in various domains of border management activities are being increasingly undertaken, with these ranging from predicting population movements in the Mediterranean and Aegean Seas by monitoring social media activities to applying artificial intelligence (AI) for risk-scoring purposes.[7]

These changes also concern the actors involved in actual border management. While border management has been first and foremost entrusted with specially trained state officials (see e.g. Article 16 Schenghen Borders Code), due to the progressive externalisation and privatisation of border control (see *infra*), the role of non-national state actors, such as private companies (e.g. air carriers) and even individuals, as well as of supranational and international actors, such as the EU and its many agencies (e.g. Frontex), and even third countries, has increased.[8] At the same time, the technologisation of border control has amplified the importance of technology providers.[9] The proliferation of technology and data actors has led to an increasingly complex regulatory framework governing border management in the EU, triggering at the same time criticism due to its possible detrimental effects on fundamental rights, particularly data protection and privacy (see *infra*) and, consequently, on democracy and the rule of law. These three elements are inherently and indivisibly linked. While each one seems to operate independently of the others, separating them in practice risks causing the system of values enshrined in Article 2 Treaty on the European Union (TEU) to collapse.[10]

The purpose of this Chapter is to support assessors in mapping the relevant legal and regulatory framework applicable to border control technologies and, therein, to emphasise those legal requirements – grouped into the three categories of data protection, privacy and ethics[11] – that have to be complied with in order to assure, to the highest extent possible, that border control technologies remain aligned with democratic principles, the rule of law and fundamental rights.

Border management law, which encompasses a patchwork of European, national and international legal and otherwise regulatory instruments (see *infra*), represents a *sui generis* component of the benchmark against which border control technologies have to be assessed under the integrated impact assessment process as proposed in this textbook. Within this process, unlike the other elements of the benchmark (namely data protection, privacy, ethics and social acceptance), border management law is not *per se* a societal concern, but rather contains provisions that do protect societal concerns. In other words, from border management law, it is possible to extrapolate legal requirements enshrining data protection, privacy and ethics that, to be lawful, border control technologies must abide by. The adherence to these requirements is expected to enhance the social acceptance of the technology under assessment.

The structure of this Chapter is as follows: Sections 7.1.2 and 7.1.3 will illustrate some of the fundamental rights and other societal concerns that can be affected by border management laws and policies, as well as by border control technologies. Section 7.2 will delve into the historical development of border management law and policies in the EU. Section 7.3 will provide an overview of the legal and regulatory instruments regulating

border management law. Section 7.4 will focus on the actors involved in border management, and, finally, Section 7.5 will overview the data protection, privacy and ethics requirements enshrined in multiple components of EU border management law that may be relevant for the integrated impact assessment process.

Border management laws and policies are instilled with certain values of a society, values that vary depending on geopolitical and historical circumstances.[12] In other words, border management activities, policy goals and necessities are fluid and subject to change over time. They may promote the respect of fundamental rights, democracy and the rule of law, or conversely advance xenophobic and racially discriminatory ideologies.[13] Given that border management is so heavily politicised, it is natural to assume that the utilisation of border control technologies is not neutral either.[14]

7.1.2 How border management laws and policies affect fundamental rights: the case of EU large-scale databases and their interoperability

Several fundamental rights and other societal concerns can be affected by border management laws and policies, as well as by border control technologies. This Section will illustrate some of them, using as a reference point the EU policies concerning large-scale databases and their interoperability that exist.

Such EU large-scale databases presently include: the second-generation Schengen Information System (SIS II), the Visa Information System (VIS), the European Dactyloscopy (Eurodac), and the more recent Entry-Exit System (EES), European Criminal Records Information System for Third Country Nationals (ECRIS-TCN) and European Travel Information and Authorisation System (ETIAS). The EU established these with the aim of supporting border guards in controlling the external borders of the Schengen Area.[15]

In a nutshell, the SIS allows competent authorities in the EU to issue and consult alerts on missing or wanted objects and people. The VIS supports Member States' consular authorities in the management of applications for short-stay visas to visit or to transit through the Schengen Area. The Eurodac supports competent authorities in determining the responsibility for examining an asylum application. In the near future, the EES will electronically register the time and place of entry and exit of third-country nationals, both those requiring a visa and those who are visa-exempt, admitted for a short stay, other than those refused to entry. The ECRIS-TCN will allow Member States' authorities to identify which other Member States hold criminal records on the third-country nationals or stateless persons being checked. The ETIAS will constitute a pre-travel authorisation system for visa-exempt travellers, the key function of which is to verify if a third-country national meets entry requirements before travelling to the Schengen Area, enabling pre-travel assessment of irregular migration, security or public health risks.[16]

Although each EU large-scale database has its purposes and specificities,[17] their technical architectures are similar. They are composed of a central system, managed by the

European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), a backup, a national system/interface in each Member State that communicates with the central one, and an (encrypted) communication infrastructure connecting them. National copies of the central system are foreseen for the SIS. All of these databases rely on the extensive processing of personal data, including biometric data (namely, fingerprints, palmprints, facial images, DNA profiles. Note that each database contains different types of biometric data).[18] It has been esteemed that the SIS contains over 70 million alerts, the Eurodac more than 5 million fingerprint datasets, and the VIS over 17 million visa applications.[19]

The official goal of the latest EU policies is that these databases will become interoperable. This interoperability scheme will build upon four components: a European Search Portal (ESP), allowing competent authorities to search multiple EU information systems simultaneously (including certain Europol data and Interpol databases).[20] This common search protocol will use biographical and biometric data; a shared biometric matching service (BMS), enabling the search and comparison of biometric data (fingerprints and facial images) from several systems that store biometric templates; a common identity repository (CIR), containing biographical and biometric data of third-country nationals recorded in the Eurodac, VIS, EES, ETIAS and ECRIS-TCN; and a multiple-identity detector (MID), which checks whether the biographical identity data contained in the search exists in other parts of the shared system, thus allowing the detection of multiple identities linked to the same set of biometric data.[21]

Many fundamental rights are affected by these EU large-scale databases and their interoperability. Various actors, including the European Data Protection Supervisor (EDPS), the EU Agency for Fundamental Rights (FRA), NGOs and academia have noted, *inter alia*, that the processing of large amounts of personal data not only jeopardises the rights to privacy and personal data protection, but may have a larger impact on democracy and society as a whole. In particular, privacy, they argue, is an inherent value in liberal democratic and pluralist societies, in addition to being a cornerstone for the enjoyment of fundamental rights.[22]

However, other fundamental rights, in particular the right to non-discrimination, are affected by these databases and their interoperability. As these databases mainly contain the data of third-country nationals, concerns have been raised over the fairness of EU laws and policies towards third-country nationals. The Court of Justice of the European Union (CJEU), albeit in a different context, highlighted that the coexistence of different data processing practices for nationals and for non-national EU citizens may be discriminatory.[23] Certain analysts even doubt the legality of having different data processing practices for EU and non-EU citizens and whether this respects the essence of the right to personal data protection.[24] Other challenges derive from the technical architecture of the databases, which renders them prone to fragilities (e.g. technical failures, errors in software configurations, discrepancies between the central system and national copies, data quality of the entries, depending mostly on the work practices of their end users).[25] In addition to jeopardising the efficiency of the IT systems, some of these fragilities affect the rights of individuals whose data are stored in them. For instance, inaccuracy of data

or discrepancies between information stored national and central systems may lead to unjust administrative decisions against a person. The negative consequences of data inaccuracy are likely to be amplified by the impending interoperability of the EU large-scale databases. When combined with interstate trust, interoperability may legitimise national authorities to blindly rely on data stored in EU data systems, even when not accurate and up-to-date, instead of performing a careful examination of each case.[26]

Furthermore, interoperability entails much more than interconnecting IT systems. It also implicates semantic, social, cultural, economic, organisational and legal issues.[27] Perhaps most importantly, far from being just a technical choice, interoperability entails a political approach that somehow blurs the lines between various policy goals (e.g. asylum, migration management, law enforcement, counterterrorism), risking, for example, a conflation of the notions of "terrorist" or "criminal" used in public discourse with the legally defined notion of "foreigner" or "alien".[28] The interconnection of technologies (and databases) also gives rise to the possibility of function creep, which could imply the expansion of surveillance and data collection functions into areas where they conflict with core data protection principles such as lawfulness, purpose limitation or data minimisation.[29]

EU laws and policies related to EU large-scale databases and interoperability are not alone in facing criticism. Another phenomenon that has been put into question is the externalisation of border control, which refers to a "range of processes whereby European actors and Member States complement policies to control migration across their territorial boundaries with initiatives that realise such control extra-territorially and through other countries and organs rather than their own".[30] The externalisation of border control has been deemed particularly detrimental to the effective exercise of the right to asylum and the principle of non-refoulement.[31]

7.1.3 How border control technologies affect fundamental rights

Just as border management laws and policies embed certain values of a society, so are border control (and digital) technologies unneutral. They can be deployed both to promote the respect of fundamental rights, democracy and the rule of law and, conversely, to advance xenophobic and racially discriminatory ideologies.[32] Border control technologies are multiple and diverse. As a general rule, they may facilitate both border checks and border surveillance activities. Border control technologies aimed at facilitating border checks primarily target individuals and rely on extensive personal data processing, whereas those used for border surveillance purposes focus on detecting events where individuals and groups are involved, which entails different risks for fundamental rights.[33]

For instance, although border control technologies may not always rely on personal data processing, there is a risk that they will jeopardise other fundamental rights, *inter alia*, the right to asylum and to non-refoulement,[34] as well as the rights of minorities, who may inadvertently become the main target groups of border surveillance activities.[35]

One form of border control technology that is particularly challenging from a fundamental rights perspective is the use of algorithmic profiling. In the context of border management, profiling is used mainly to identify known individuals based on previously collected data or as a predictive method to identify unknown individuals who may be of interest to border management authorities,[36] on the basis of risk indicators.[37] EU large-scale databases (in particular, the ETIAS) have come to increasingly incorporate algorithmic decision-making, including profiling functionalities (e.g. to determine whether an individual is to be determined a risk).[38] By analysing existing data derived from past experiences and statistical analysis, correlations between certain characteristics and particular outcomes or behaviours are established and used to draw conclusions, and make decisions about certain individuals.[39] Consequently, whereas profiling can be a useful tool, its use may lead biased outcomes, affecting, *inter alia*, equality, non-discrimination, privacy and data protection.[40]

Equality and non-discrimination are also at stake, considering that the accuracy of certain border control technologies (e.g. facial recognition) relative to parameters such as gender and skin tone, may give rise to discrimination.[41] Border control technologies are, in this sense, prone to perpetuate human rights harms and exacerbate systemic discrimination.[42]

The performance of the integrated impact assessment of border control technologies can help to minimise such negative consequences.

7.2 The historical development of border management law in the EU

As mentioned above, the essential twofold goal of border management (law) is to facilitate the efficient flow of *bona fide* travellers while preventing the entry of irregular travellers.[43] To achieve this objective, multiple approaches are possible.

For centuries, the so-called "nationalist approach" towards border control has been predominant in Europe.[44] In a nutshell, such an approach, typical of modern states, conceives border control as a corollary of sovereignty and therefore a purely domestic matter, for which national governments are the sole responsible actors.[45] The so-called Westphalian (or modern) state system builds upon the idea that sovereign states possess the monopoly of force within their mutually recognised territories, which are delimited by borders.[46] Considering that sovereignty for a state entails having control over the territory, the population and the goods therein, borders function as a kind of "filter", demarcating "a portion of the globe that a centralised authority claims as its own and to protect it from external threats".[47] Centuries after the Treaties of Westphalia (1648), the Montevideo Convention on the Rights and Duties of States (1933) still considers the territory, enclosed within borders, as a statehood criterion, together with population, government, and the capacity to enter into relations with other states.[48]

With the emergence of supranational institutions, the concept of sovereignty transformed. In Europe, with the process of European integration, the Member States of what is today known as the European Union (EU), started to transfer the execution of some of their sovereign competences at a supranational level, including those competences that relate to border management.[49] This conferral of these competences is a direct consequence of the emergence of the Common Market and four freedoms of the EU, namely the freedom of movement of goods, persons, services, capitals (Title IV TFEU), which are, in turn, safeguarded by diverse policies within the Area of Freedom, Security and Justice (AFSJ), pertaining to, for example, migration (Title V TFEU).

In the process of European integration, supranational cooperation has progressively acquired more and more power and competences in the field of border management. The signing of the Schengen Agreement (1985) and of the Convention Implementing the Schengen Agreement (1990) have laid the foundation for the gradual abolition of internal border controls, homogenisation of visa policies, and implementation of a cooperating structure between internal and immigration officers, including the establishment of the Schengen Information System.[50] Yet, the two were international agreements, valid exclusively among the signatory states. The Treaty of Maastricht (1992), establishing the so-called three-pillars structure for the organisation of the competences of the European Union,[51] introduced for the first time the idea of European cooperation in the field of border management, although still based on inter-governmentalism.[52] The Treaty of Amsterdam (1997) went further by incorporating the Schengen rules, previously applicable only to the signatory states of the Schengen Agreement and the Convention implementing it, into the *acquis communautaire*; the body of common rights and obligations that are binding for all EU countries, as EU Member States.[53] With the Treaty of Lisbon (2007) and the abolition of the pillars structure, the intergovernmental approach in the field of border management was overcome, border management being nowadays entirely reconducted to supranational cooperation.[54]

Border management laws and policies in the EU build upon the assumption that, to ensure a high level of security and the freedom of movement within the EU, one of the necessary conditions is the strong and reliable (integrated) management of the movement of persons across external borders.[55] The progressive technologisation and digitalisation that has come to characterise the EU policies of recent decades is precisely intended to better-secure the EU's external borders and streamline border crossing by becoming increasingly reliant on automated information-sharing and self-service.[56]

These developments represent a turning point in comparison to the above-mentioned nationalist approach.[57] Although the EU system still acknowledges the existence of national borders and maintains the rhetoric of borders as filters against external threats, it introduces a key novelty, namely the distinction between internal and external borders. Whereas for the former, the controls are in principle lifted, i.e. these borders may be crossed at any point without a border check on persons – irrespective of their nationality – being carried out,[58] for the latter, controls are in place and – what is perhaps more important – a common policy is established.[59]

This distinction affects also the perception that individuals have about borders and the EU as a whole. From the insider's perspective, the EU may appear open and hospitable, whereas for the rest of the world, it may appear more closed, secure and less permissive.[60] Internal borders are deemed rather inclusive and less visible, while external borders are perceived as exclusive and restrictive, since security and border traffic control are transferred thereto.[61]

7.3 Legal and regulatory instruments governing border management in the EU

Nowadays, border management in the EU is governed by a patchwork of legal and otherwise regulatory instruments, encompassing European primary law sources, namely the Treaties (Treaty on the European Union (TEU) and Treaty on the Functioning of the European Union (TFEU)), and the Charter on Fundamental Rights of the European Union (CFR). While Article 3(2) TEU states the essence thereof – namely that the "Union shall offer its citizens an area of freedom, security and justice without internal frontiers, in which the free movement of persons is ensured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime", Title V TFEU on the Area of Freedom Security and Justice further specifies a common policy on asylum, immigration and external border control, all of which must conform to the CFR; when implementing EU law, Member States are also bound by the Charter.

Secondary law sources, such as regulations, directives and (implementing) decisions, also play a role in framing EU border management policy. This includes, first and foremost, a legal statute for each border management tool, ranging from Schengen through large-scale databases and their interoperability, the Passenger Name Record (PNR) Directives, the Advanced Passenger Information (API) Directive, the European Border Surveillance System (Eurosur), the rules governing the European bodies and agencies, the rules governing border control of persons crossing the external borders of the Member States of the Union (contained in the Schengen Borders Code (SBC)), to identity cards and passports, unmanned air vehicles, dual-use, etc.[62]

In addition to EU law, Member States are bound by public international law instruments, e.g. bilateral agreements, treaties and conventions, such as the 1950 European Convention on Human Rights, the 1951 Geneva Convention, and the 1967 Protocol Relating to the Status of Refugees. National laws play a role insofar as certain matters, directly or indirectly linked to border management, such as intelligence, military and internal security, are the exclusive competence of Member States.[63]

Eventually, soft law instruments, such as internal policies and practices of border authorities and memoranda of understanding concluded between border control authorities of

neighbouring countries, also come into play in the formation of policy. Finally, a number of technical standards fixed for biometric data contained in passports (International Civil Aviation Organisation (ICAO), National Institute of Standards and Technology (NIST)) set certain limitations on the implementation of border management policy.

7.4 Actors involved in border management in the EU

Over recent decades, border management has come to no longer be a prerogative of state actors alone. The actors currently involved, directly or indirectly, in border management activities can be grouped into three main categories, namely national state actors, supranational state actors (in this context, the EU and its institutions, bodies, offices and agencies) and private actors.

National state actors include the border control authorities entrusted with the actual performance of border checks and border surveillance under national and/or EU law, national law enforcement agencies, insofar as they are assigned border management-related tasks, Passenger Information Units (PIUs) established under the Passenger Name Records (PNR) Directive, and national Data Protection Authorities (DPAs), to the extent that they oversee how nationally competent authorities use EU large-scale databases.

Amongst supranational state actors, apart from the Commission, the European Parliament and the Council, several EU bodies and agencies have been set up and tasked with border management tasks. The European Border and Coast Guard Agency (commonly known as Frontex)[64] , together with Member States' responsible authorities, oversees the effective implementation of integrated border management at the external borders of the EU. The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA) is in charge of the operational management of the SIS, VIS and Eurodac, and of the preparation, development and operational management of EES, ETIAS and ECRIS-TCN.[65] The European Data Protection Supervisor (EDPS) has responsibility for supervising personal data processing in the central units of the databases hosted by eu-LISA (the EDPS and national DPAs form together the Supervision Coordination Groups (SCGs)).[66] The European Asylum Support Office (EASO) contributes to the development of the Common European Asylum System by facilitating, coordinating and strengthening practical cooperation among Member States on the many aspects of asylum.[67] Finally, the European Union Agency for Law Enforcement Cooperation (Europol) will, under certain conditions (e.g. when necessary to fulfil its mandate), have access to the SIS, VIS, Eurodac, EES, ETIAS and ECRIS-TCN.[68]

Private actors include carriers and those private entities that, due to the progressive privatisation of border control, have been tasked with specific border management-related tasks such as sharing passenger-related information with border control authorities or denying boarding.[69] A key group of private actors not mentioned in the legal and otherwise regulatory framework, but that in practice influence border management, are the technology

providers themselves.[70] When public authorities lack the technical capacity for deploying and understanding border control technologies, they may rely, sometimes to a high degree, on technology developers. This has a tendency to enable these private actors to influence the border control agenda and to shape priorities regarding the technologies to be deployed.[71]

7.5 Legal requirements enshrining data protection, privacy and ethics in EU border management law

7.5.1 An introduction to the built-in safeguards system of EU border management law

Given the EU's commitment to democracy, the rule of law and fundamental rights, border management law in the EU contains built-in safeguards that protect these values, and in particular data protection, privacy and ethics. Therefore, for the purposes of the process of integrated impact assessment of border control technologies, these requirements enshrining data protection, privacy and ethics have to be evaluated by means of a legal compliance check on the envisaged technology. The adherence to these requirements is further expected to enhance the social acceptance of the technology under assessment.

It should be noted that the sole legal compliance check against data protection, privacy and ethics requirements does not necessarily grant that a border control technology is socially acceptable and respects democracy, the rule of law and fundamental rights. Indeed, as mentioned above, border management laws (and policies) may embed xenophobic and racially discriminatory ideologies. In democratic systems, many safeguards are arguably in place to avoid this happening. For instance, at a procedural level, part of the EU framework governing border management (e.g. regulations, directives) is the outcome of the ordinary legislative procedure,[72] where the European Parliament is co-legislator with the Council. Yet, this does not automatically ensure the adherence of these laws to superior sources (e.g. Charter of Fundamental Rights of the European Union). The EU legal framework can be challenged in front of the Court of Justice of the European Union and invalidated. In other words, procedural democracy does not necessarily coincide with substantive democracy, which functions with the actual interest of those governed.[73] Furthermore, when legislation is adopted specifically to confront emergency situations, using an intergovernmental method,[74] or has (apparently) more technical content (e.g. EU implementing and delegated acts), the democratic scrutiny is lessened.[75] Similar considerations are valid, *mutatis mutandis*, for national laws governing border management.

Each type of technology to be implemented corresponds to an applicable legal framework. For example, when border control technologies are used to perform border checks, they may be connected to EU large-scale databases, meaning that rules on EU large-scale databases and the Schengen Borders Code are applicable, and compliance requirements

must be extrapolated therefrom. Conversely, when border control technologies are aimed at performing border surveillance activities, other rules (Eurosur) may be relevant. (An inventory of the EU legal framework potentially applicable to border control technologies, grouped into macro-topics, is provided in Annex IV of this textbook.)

As a general rule, the legal framework applicable to border control technologies, and particularly in regard to the exchange of information in border management activities (e.g. EU large-scale databases, interoperability regulations), is governed by its own data protection rules (*lex specialis*). Matters that are not expressly regulated in the framework are referred mainly to the General Data Protection Regulation (GDPR) (*lex generalis*), unless the purpose is "the prevention, detection or investigation of terrorist offences or other serious criminal offences", meaning that the Law Enforcement Directive (LED) is applicable.[76]

For the European institutions, bodies and agencies involved in border management, the *lex generalis* is Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data (EUDPR). Chapter IX EUDPR regulates the processing of operational personal data by Union bodies, offices and agencies when carrying out activities falling within the scope of judicial cooperation in criminal matters and police cooperation. Certain regulations establishing EU bodies and agencies contain their own data protection rules that constitute *lex specialis* in relation to the EUDPR (for Frontex, this is, for example, Chapter IV, Section 2 Frontex Regulation). Europol is an exception to this, due to the fact that, at present, it has its own data protection rules.

More specifically, border management law establishes some special rules, especially in relation to data subjects' rights, data transfers, accessibility of personal data and accuracy of biometric data, that specify the *lex generalis*. In addition, border management law gives substance and further specifies certain concepts contained in the GDPR (e.g. allocation of roles of controllers and processors). Regarding other obligations (e.g. the need to appoint a data protection officer (DPO), the requirement for the data controller to perform a DPIA), border management authorities and EU bodies and agencies involved in border management are still bound by the GDPR, the LED and/or the EUDPR.

7.5.2 Summary of the data protection, privacy and ethics requirements of the EU border control system

7.5.2.1 Data Protection Requirements

The following is a cursory overview of the specific regulatory measures current assured by multiple components of EU border management law. This Section needs to be read in conjunction with Chapter 4 on personal data protection, where the concepts under the *lex generalis* are presented.

1. *Roles of controllers and processors*. The responsibilities of controllers and processors are allocated in accordance with the law.

In some cases, border management law expressly allocates the roles of controllers and processors in the entities involved in data processing operations.[77] The distinction is important because data controllers have broader obligations than data processors (e.g. performance of a DPIA).[78]

2. *Lawful processing*. A legal basis grounds the personal data processing performed by the border control technology.
   Border management law may lay down the basis for certain processing operations (e.g. expressly require border control authorities to carry out certain data processing operations), or clarify the legal basis to be used in certain processing (e.g. consent).[79]
3. *Purpose limitation*. Data processed by a border control technology are processed for specified, explicit and legitimate purposes, in line with those specified in the relevant legal and regulatory framework applicable to it.
   Border management law lists the purposes for which a border control activity is carried out and personal data are to be processed (e.g. each EU large-scale IT system has own purposes, whereas the PNR and API directives specify why PNR and API are processed).[80] Therefore, when a border control technology processes personal data, the purposes of processing need to be in-line with those specified in the legal framework applicable to it.
4. *Data minimisation*.
   4.1. The border control technology processes only the personal data that are adequate, relevant and not excessive for the specific border control activity.
   In the context of border management, not all the activities performed by border control authorities require personal data processing. Border management law clarifies that, whereas personal data processing is a core function for border checks,[81] it is conversely exceptional for border surveillance.[82]
   4.2. The border control technology ensures that only certain categories of personal data are processed.
   While a border control technology may have the technical capacity to process multiple categories of personal data, not all of them are necessary for performing a border management activity. For example, border management law provides a closed list of the categories of personal data that can be stored/processed in EU large-scale databases,[83] or collected and transferred by (air) carriers.[84]
5. *Accuracy*. Mechanisms are in place to ensure that data processed by a border control technology are accurate and up-to-date, and that any change in the data is promptly communicated to those (authorities) concerned.
   Keeping data accurate and up-to-date in the context of border management is of utmost importance to effectively take action against those individuals that represent a threat to security and to prevent unjust decisions against *bona fide* individuals.[85] Accordingly, border management law requires border control authorities to set up mechanisms to ensure that inaccurate or outdated information stored in a database is erased or updated within a specific period of time, and that the changes are communicated to those (authorities) concerned.[86]

6. *Accuracy for biometric data*. The border control technology complies with minimum data quality standards for biometric data.
   Border management law adopts a (partially) different approach compared to the *lex generalis* on biometric data. Whereas under the *lex generalis* the processing of biometric data is in principle prohibited, it is conversely the core of the functioning of EU large-scale IT systems and portrayed as a more secure, efficient and reliable solution for identification and verification of the identity of individuals.[87] However, for reliable identification and verification of identities, the accuracy of biometric data is of pivotal importance. For this reason, border management law expressly sets standards for the accuracy of biometric data that border control technologies must comply with.[88]
7. *Storage limitation*.
   7.1. The border control technology ensures that data are automatically deleted once the retention period elapses.
   Border management law expressly defines the data retention period for the information stored in EU large-scale databases and of the personal data processed by Frontex. As a further safeguard for the data subjects, it requires that, once the data retention period elapses, data are automatically deleted.[89]
   7.2. The border control technology ensures that log data are deleted once the retention period elapses.
   Border management law specifies the retention period for logs in relation to both EU large-scale databases and their interoperability. However, since logs are kept for accountability purposes (see *infra*), their deletion is not automatic.[90]
8. *Data security (availability, integrity & confidentiality)*. The organisation adopts technical and organisational measures to ensure the security of the data processed by the border control technology.
   Border management law expressly introduces certain technical and organisational measures that that need to be complied with to ensure, to the greatest extent possible, the security and availability of EU large-scale databases. Such organisational measures include the establishment of a security plan, a business continuity plan and a disaster recovery plan, as well as fall-back procedures.[91] The technical measures include the encryption of the communication infrastructure connecting national interfaces and central systems, and measures ensuring the technical compatibility between national interfaces and central systems for the transmission of data.[92]
9. *Accountability*. The border control authority has accountability measures in place.
   Border management law provides for a series of accountability measures that include:
   - maintenance of logs/records of processing activities (which are also made available to supervisory authorities);[93]
   - staff training on data protection and rules and procedures of processing;[94]
   - self-monitoring of the national and EU authorities dealing with EU large-scale databases;[95]

- requirements that that persons working with EU-large scale databases are bound by professional secrecy or equivalent;[96]
- requirements as to what documentation (e.g. records of data subjects' requests, inventories of technical copies of databases, reports of security incidents)[97] is made available to supervisory authorities.

10. *Data subjects' rights*. Data subjects are granted the possibility to exercise their rights.
Data subjects' rights have been developed with the aim of mitigating the power imbalances between data controllers and data subjects, to enhance the control of the latter over their personal information.[98] In law enforcement and security-related contexts, they are more limited in scope but still need to be granted.[99] Similarly, border management law poses some limitations, but still ensures that data subjects enjoy the rights to:
    - information;[100]
    - access (also indirect via a DPA);[101]
    - rectification;[102]
    - erasure;[103]
    - restriction of processing (for EES, ETIAS, ECRIS-TCN, MID);
    - to a certain extent, not to be subject to a decision based solely on automated processing that significantly affects them.[104]

    Border control authorities need to keep track of data subjects' requests, reply to them within the deadlines specified in the legal framework applicable to them and, in the event that they are unable to comply with the request, inform data subjects of the reasons for refusal and of their right to lodge a complaint with a DPA. Together with eu-LISA, they are liable for damages suffered by individuals resulting from unlawful data processing.[105]
11. *Data transfers*. Transfers to third countries and/or international organisations of data collected by the border control technology is either not allowed or restricted to very specific cases.
    Border management law adopts a special approach towards data transfer compared to the *lex generalis*. Data transfers to third countries are forbidden or limited to very specific cases. This is due to the fact that the sharing of personal data with third countries could be particularly dangerous for those seeking international protection.[106] Restrictions are also in place regarding transfers to international organisations and private entities.[107]
12. *Accessibility of personal data*.
    12.1. Only specific staff members of pre-defined national competent authorities have access to data processed by the border control technology.
    12.2. Only specific staff members of pre-defined EU agencies have access to data processed by the border control technology insofar as it is necessary for fulfilling their mandate or performing their tasks.
    Preventing unlawful access in the context of border management is a pressing issue considering the possibilities of function creep brought about by the inter-

operability of EU large-scale databases.[108] This is why border management law ensures, on the one hand, that only specific staff members of pre-defined national competent authorities have access to data processed by the border control technology,[109] and, on the other, that only specific staff members of pre-defined EU agencies have access to data processed by the border control technology insofar as it is necessary to fulfil their mandate or perform their tasks.[110]

7.5.2.2 Privacy and ethics requirements

Border management law sets out provisions neither on ethics nor the protection of privacy or private life are scarce.

It should be noted that privacy and ethics requirements are inferred from the broader requirement to ensure, in the course of border management activities, the protection of fundamental rights. As mentioned above, ethics (and privacy) requirements still remain legal requirements. Yet, ethics requirements have been defined in this way because compliance with them might be requested by ethics committees or similar expert bodies.

Privacy Requirements

1. *Respect of one's private life*. The border control technology ensures that the processing of personal data respects one's private life.
   Border management law requires that the processing of personal data respects one's private life.[111]
2. *Respect of (body) integrity*. The border control technology ensures that the processing of personal data respects the (body) integrity of individuals.
   Border management law requires that processing of personal data respects the (body) integrity of individuals.[112]
3. *Privacy by design*. Privacy considerations have been embedded in the border control technology for its entire lifecycle.
   Border management law requires that data privacy considerations are embedded in the border control technology for its entire lifecycle.[113] This requirement derives from the need for eu-LISA to follow the principles of privacy by design and by default throughout the entire lifecycle of the development of the EES.
4. *Privacy by default*. The default settings of the border control technology are the most privacy-friendly possible.
   Border management law requires that the default settings of the border control technology are the most privacy-friendly possible.[114] This requirement derives from the need for eu-LISA to follow the principles of privacy by design and by default throughout the entire lifecycle of the development of the EES.

Ethics requirements

1. *Informed consent.*
   1.1. The public is informed about the existence of the border crossing point.[115]
   1.2. The public is informed of the temporary reintroduction of border controls.[116]

2. *Freedom of choice.*
   2.1. Persons may opt to not use a border control technology (e.g. e-gate).[117]
   2.2. Persons who opt to not use a border control technology (e.g. e-gate) are not discriminated against for their choice.[118]
3. *Dual-use.*
   Border management law sets restrictions on dual-use border control technologies (e.g. limitations to their export, transit and brokering).[119]
4. *Fairness.*
   The use of the border control technology is fair towards third-country nationals. This requirement derives from the need of EU policies to be fair towards third-country nationals.[120]
5. *Human dignity.*
   5.1. The use of the border control technology does not result in inhuman or degrading treatment. This requirement derives from the need for border control to not result in inhuman or degrading treatment.[121]
   5.2. Fingerprinting is in accordance with safeguards in the CFR.[122]
6. *Non-discrimination and bias.*
   The processing of personal data shall not result in discrimination against persons on any grounds.[123]
7. *Rights of elderly and people with disabilities.*
   Border control technologies are designed to be used by all persons, except for children under 12 years of age.[124]
8. *Rights of children.*
   8.1. Children under a certain age are exempted from providing fingerprints.[125]
   8.2. Border control alerts regarding children are admissible only in restricted cases, and with the aim of safeguarding the best interests of the child.[126]
   8.3. Alerts concerning children are deleted when the child reaches the age of majority.[127]
   8.4. Queries in the CIR against minors of 12 years of age are forbidden unless in the best interests of the child.[128]
9. *Vulnerable persons.*
   9.1. Alerts concerning vulnerable persons are admissible only in restricted cases.[129]
   9.2. Alerts concerning vulnerable persons are deleted in certain circumstances.[130]
   9.3. Border guards have received specialised training for detecting and dealing with situations involving vulnerable persons.[131]
10. *Non-refoulement and right to asylum.*
   10.1. Regardless of the use of a border control technology, individuals are not subject to refoulement and have the possibility to request asylum.[132]
   10.2. Particular attention is to be paid to the rights of people in need of international protection.[133]

Endnotes

1. Berry Tholen, "The Changing Border: Developments and Risks in Border Control Management of Western Countries," *International Review of Administrative Sciences* 76, no. 2 (2010): 259–78, https://doi.org/10.1177/0020852309365673; Evelien Brouwer, "Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection," *European Public Law* 26, no. 1 (2020): 71–92.
2. Nadav Morag, "Border Management in Europe: Is the Paradigm Evolving?," *Homeland Security Affairs* 16, no. 1 (2020). Recital 1 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624, OJ L 295, 14.11.2019, 1–131 (Frontex Regulation). See also Recital 6 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 77, 23.3.2016, p. 1–52.
3. Gloria González Fuster and Serge Gutwirth, "When 'Digital Borders' Meet 'Surveilled Geographical Borders': Why the Future of EU Border Management Is a Problem", in *A Threat against Europe. Security, Migration and Integration*, eds. J. Peter Burgess and Serge Gutwirth (Brussels: VUBPress, 2011), 171–90.
4. Tholen, "The Changing Border: Developments and Risks in Border Control Management of Western Countries."
5. Gloria González Fuster, Paul De Hert, and Serge Gutwirth, "Privacy and Data Protection in the EU Security Continuum," *INEX Policy Brief* 12 (2011).
6. González Fuster and Gutwirth, "When 'Digital Borders' Meet 'Surveilled Geographical Borders': Why the Future of EU Border Management Is a Problem."
7. Petra Molnar, EDRi, and the Refugee Law Lab, "Technological Testing Grounds – Migration Management Experiments and Reflections from the Ground Up," 2020.
8. Tholen, "The Changing Border: Developments and Risks in Border Control Management of Western Countries."
9. Diego Naranjo and Petra Molnar, "The Privatization of Migration Control," 2020.
10. Sergio Carrera, Elspeth Guild, and Nicholas Hernanz, "The Triangular Relationship between Fundamental Rights, Democracy and the Rule of Law in the EU Towards an EU Copenhagen Mechanism", CEPS Paperbacks, 2013.
11. Although the benchmark for the integrated impact assessment is quadripartite, the legal requirements were grouped into the three categories of data protection, privacy and ethics because border management law does not contain provisions enshrining social acceptance.
12. Zaiotti refers to different 'cultures of border control' defined as "relatively stable constellation[s] of background assumptions and corresponding practices shared by a border control community in a given period and geographical location". Ruben Zaiotti, *Cultures of Border Control: Schengen and the Evolution of European Frontiers* (Chicago: University of Chicago Press, 2011).
13. Tendayi Achiume, "Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance," 2020.
14. Achiume.
15. European Court of Auditors, "Special Report EU Information Systems Supporting Border Control-a Strong Tool, but More Focus Needed on Timely and Complete Data," 2019.
16. The EES, ETIAS and ECRIS-TCN are foreseen to be established by 2023. Diana Dimitrova and Teresa Quintel, "Technological Experimentation Without Adequate Safeguards? Interoperable EU Databases and Access to the Multiple Identity Detector by SIRENE Bureaux," *Data Protection and Privacy, Volume 13, Data Protection and Artificial Intelligence*, eds.,

Dara Hallinan, Ronald Leenes, and Paul De Hert (Oxford: Hart Publishing, 2021). See Glossary for further information.

17. For an overview of the main objectives of each EU large-scale database: European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights* (Luxembourg: Publications Office of the European Union, 2018), https://doi.org/10.2811/29.
18. Teresa Quintel, "Connecting Personal Data of Third Country Nationals: Interoperability of EU Databases in the Light of the CJEU's Case Law on Data Retention," *University of Luxembourg Law Working Paper* 2 (2018); Simone Casiraghi and Alessandra Calvi, "Biometric Data in the EU (Reformed) Data Protection Framework and Border Management," in *Personal Data Protection and Legal Developments in the European Union*, ed. Maria Tzanou (Hershey: IGI-Global, 2020), 202–23, https://doi.org/10.4018/978-1-5225-9489-5.ch010.
19. European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights*.
20. I.e. the Interpol Stolen and Lost Travel Document database (SLTD database) and the Interpol Travel Documents Associated with Notices database (TDAWN database).
21. Katrien Luyten and Sofija Voronova, "Interoperability between EU Border and Security Information Systems," 2019.
22. European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights*.
23. González Fuster, De Hert, and Gutwirth, "Privacy and Data Protection in the EU Security Continuum."
24. Brouwer, "Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection."
25. Rocco Bellanova and Georgios Glouftsios, "Controlling the Schengen Information System (SIS II): The Infrastructural Politics of Fragility and Maintenance," *Geopolitics* 24, no. 2 (2020): 1–25, https://doi.org/10.1080/14650045.2020.1830765.
26. Evelien Brouwer, "Interoperability of Databases and Interstate Trust: A Perilous Combination for Fundamental Rights," Verfassungsblog.de, 2019.
27. Paul De Hert and Serge Gutwirth, "Interoperability of Police Databases within the EU: An Accountable Political Choice?," *International Review of Law, Computers & Technology* 20, no. 1–2 (2006): 21–35, https://doi.org/10.1080/13600860600818227.
28. EDPS Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems, Brussels, 16 April 2018.
29. Tim Dekkers, "Technology Driven Crimmigration? Function Creep and Mission Creep in Dutch Migration Control," *Journal of Ethnic and Migration Studies* 46, no. 9 (2020): 1849–64, https://doi.org/10.1080/1369183X.2019.1674134.
30. Violeta Moreno-Lax and Martin Lemberg-Pedersen, "Border-Induced Displacement: The Ethical and Legal Implications of Distance-Creation through Externalization," *QIL, Zoom-In* 56 (2019): 5–33.
31. Bill Frelick, Ian M. Kysel, and Jennifer Podkul, "The Impact of Externalization of Migration Controls on the Rights of Asylum Seekers and Other Migrants," *Journal on Migration and Human Security* 4, no. 4 (2016): 190–220.
32. Achiume, "Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance."
33. Rocco Bellanova and Denis Duez, "The Making (Sense) of EUROSUR: How to Control the Sea Borders?," in *EU Borders and Shifting Internal Security: Technology, Externalization and Accountability*, ed. Raphael Bossong and Helena Carrapico (Heidelberg: Springer, 2016), 23–44.
34. European Union Agency For Fundamental Rights, *How the Eurosur Regulation Affects Fundamental Rights* (Luxembourg: Publications Office of the European Union, 2018).

35. Molnar, EDRi, and the Refugee Law Lab, "Technological Testing Grounds – Migration Management Experiments and Reflections from the Ground Up."
36. European Union Agency for Fundamental Rights, *Preventing Unlawful Profiling Today and in the Future: A Guide* (Luxembourg: Publications Office of the European Union, 2018), https://doi.org/10.2811/801635.
37. Gloria González Fuster, "Artificial Intelligence and Law Enforcement" (Brussels, 2020).
38. Fondazione Giacomo Brodolini, "Fundamental Rights Review of EU Data Collection Instruments and Programmes," 2019; González Fuster, "Artificial Intelligence and Law Enforcement."
39. European Union Agency for Fundamental Rights, *Preventing Unlawful Profiling Today and in the Future: A Guide*.
40. European Union Agency for Fundamental Rights.
41. Joy Buolamwini and Timnit Gebru, 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification', in Proceedings of Machine Learning Research (Conference on Conference on Fairness, Accountability, and Transparency 2018), 2018, 1–15.
42. Molnar, EDRi, and the Refugee Law Lab, "Technological Testing Grounds – Migration Management Experiments and Reflections from the Ground Up."
43. Tholen, "The Changing Border: Developments and Risks in Border Control Management of Western Countries."
44. Zaiotti, *Cultures of Border Control: Schengen and the Evolution of European Frontiers*.
45. Zaiotti.
46. Iain McLean and Alistair McMillan, "Westphalian State System," in *The Concise Oxford Dictionary of Politics* (Oxford University Press, January 2009), https://doi.org/10.1093/acref/9780199207800.001.0001.
47. Mariano Cesar Bartolomé, "The Modern State Facing a Challenging International Security Scenario of Postwestfalian Characteristics," *Defense and Security Studies* 5, no. 5 (2008): 10–15.
48. Archie Simpson, "Nations and States," in *Issues In International Relations*, ed. Trevor C. Salmon, Mark F. Imber, and Trudy Fraser, 2nd ed. (London and New York: Routledge, 2008), 1–258, https://doi.org/10.4324/9780203926598.
49. Nathalie Brack, Ramona Coman, and Amandine Crespy, "Sovereignty Conflicts in the European Union," *Les Cahiers Du Cevipol* 4, no. 4 (2019): 3–30.
50. Saara Koikkalainen, "Free Movement in Europe: Past and Present," 2011.
51. The pillars were the European Communities (EC) pillar, aimed at implementing the single market; the Common Foreign and Security Policy (CFSP) pillar, aimed at defining and implementing a common foreign and security policy; and the Justice and Home Affairs (JHA) pillar, aimed at developing a common action in areas such as the controlling external borders and illegal migration in order ensure a high level of safety for citizens within the JHA. The main difference between the three pillars regarded the decision-making process (for the first pillar, the community method, characterised by the centrality of the role of European Institutions in the decision-making; for the second and third pillar, the intergovernmental method, requiring the consensus of governments of the single Member States and envisaging a limited role for European Institutions). Ina Sokolska, "The Maastricht and Amsterdam Treaties," 2021; General Secretariat of the Council of the European Union, *The Pillars of Europe – The Legacy of the Maastricht Treaty after 25 Years* (Brussels, 2018).
52. Youri Devuyst, "The European Union's Institutional Balance after the Treaty of Lisbon: Community Method and Democratic Deficit Reassessed," *Georgetown Journal of International Law* 2, no. 39 (2008): 247–326. General Secretariat of the Council of the European Union, *The Pillars of Europe – The Legacy of the Maastricht Treaty after 25 Years*.
53. Hilf Meinhard, "Acquis Communautaire," in *Max Planck Encyclopedia of Public International Law* (Oxford University Press, 2009), https://doi.org/10.1093/law:epil/9780199231690/e1717; Koikkalainen, "Free Movement in Europe: Past and Present."

54. Devuyst, "The European Union's Institutional Balance after the Treaty of Lisbon: Community Method and Democratic Deficit Reassessed."
55. Communication from the Commission to the European Parliament and the Council 'Stronger and Smarter Information Systems for Borders and Security' (COM/2016/0205 final)
56. Pinja Lehtonen and Pami Aalto, "Smart and Secure Borders through Automated Border Control Systems in the EU? The Views of Political Stakeholders in the Member States," *European Security* 26, no. 2 (2017): 207–25, https://doi.org/10.1080/09662839.2016.1276057.
57. Zaiotti, *Cultures of Border Control: Schengen and the Evolution of European Frontiers*.
58. Article 22 SBC. It is only exceptionally, and as *extrema ratio*, when there is a serious threat to public policy or internal security in a Member State, that a Member State may reintroduce border control at all or specific parts of its internal borders for a limited period of up to 30 days or for the foreseeable duration of the serious threat if its duration exceeds 30 days (Article 25 SBC).
59. Zaiotti.
60. Mircea Brie and Ioan Horga, "The European Union External Border: An Epistemological Approach," *Romanian Review on Political Geography*, no. 1 (2009): 15–31.
61. Brie and Horga.
62. See Annex 4 in this Volume.
63. Morag, "Border Management in Europe: Is the Paradigm Evolving?"
64. Article 5 Regulation (EU) 2019/1896 of the European Parliament and of the Council of 13 November 2019 on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 (hereafter, Frontex Regulation).
65. Regulation (EU) 2018/1726 of the European Parliament and of the Council of 14 November 2018 on the European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA), and amending Regulation (EC) No 1987/2006 and Council Decision 2007/533/JHA and repealing Regulation (EU) No 1077/2011.
66. Article 62 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.
67. Regulation (EU) No 439/2010 of the European Parliament and of the Council of 19 May 2010 establishing a European Asylum Support Office.
68. Brouwer, "Large-Scale Databases and Interoperability in Migration and Border Policies: The Non-Discriminatory Approach of Data Protection."
69. Frank Mc Namara, "Externalised and Privatised Procedures of EU Migration Control and Border Management – A Study of EU Member State Control and Legal Responsibility" (European University Institute, 2017).
70. Naranjo and Molnar, "The Privatization of Migration Control."
71. Naranjo and Molnar.
72. Legislative Affairs Unit of the European Parliament (LEGI), *Handbook on the Ordinary Legislative Procedure – A Guide to How the European Parliament Co-Legislates*, 2020.
73. Marc Bühlmann and Hanspeter Kriesi, "Models for Democracy," in *Democracy in the Age of Globalization and Mediatization* (London: Palgrave Macmillan UK, 2013), 44–68, https://doi.org/10.1057/9781137299871_3.
74. Devuyst, "The European Union's Institutional Balance after the Treaty of Lisbon: Community Method and Democratic Deficit Reassessed."
75. Thomas Christiansen and Mathias Dobbels, "Non-Legislative Rule Making after the Lisbon Treaty: Implementing the New System of Comitology and Delegated Acts," *European Law Journal* 19, no. 1 (2013): 42–56, https://doi.org/10.1111/eulj.12012; Molnar, EDRi, and the Refugee Law Lab, "Technological Testing Grounds – Migration Management Experiments and Reflections from the Ground Up."

76. Casiraghi and Calvi, "Biometric Data in the EU (Reformed) Data Protection Framework and Border Management."
77. For example, Article 40 Interoperability Regulation (EU) 2019/817 of (hereafter, Interoperability Regulation 817) and Interoperability Regulation (EU) 2019/818 (hereafter, Interoperability Regulation 818) clarifies that national authorities that are controllers, on the one hand, for the EES, VIS and SIS and, on the other hand, for the Eurodac, SIS and ECRIS-TCN respectively shall be considered controllers in relation to the biometric templates that they enter into the Shared BMS; similarly, for the data *ex* Article 18 Interoperability Regulations that they enter into the CIR. National authorities adding or modifying the data in the identity confirmation file are controllers for the processing of the personal data in the MID. Article 41 Interoperability Regulations specifies that eu-LISA is data processor for the Shared BMS, the CIR and the MID. Article 57 Regulation (EU) 2018/1240 (hereafter, ETIAS Regulation) establishes that: Frontex is considered the data controller in relation to the processing of personal data in the ETIAS Central System; the ETIAS National Unit is considered the data controller in relation to the processing of personal data in the ETIAS Central System by a Member State; eu-LISA is considered the data controller in relation to information security management of the ETIAS Central System but the data processor in relation to the processing of personal data in the ETIAS Information System.
78. Brendan Van Alsenoy, "Liability under EU Data Protection Law: From Directive 95/46 to the General Data Protection Regulation," *JIPITEC* 7, no. 3 (2017).
79. For example, Article 8 SBC establishes against which databases individuals must be controlled during border checks. Article 47 Regulation (EU) 2018/1861 (hereafter, SIS Regulation 1861) requires the consent of the person whose identity has been misused to enter and process in the SIS certain data. Similarly, Article 54 ETIAS Regulation admits that an individual may consent to have their application files stored after the expiry of ETIAS travel authorisation for the purpose of facilitating a new application.
80. Lists of the purposes for which personal data may be processed by a border control technology are contained for instance in: Articles 1, 24, 25, 41, 47, 49 SIS Regulation 1861; Articles 1, 26, 32, 34, 36, 38, 40, 56, 64 Regulation (EU) 2018/1862 (hereafter, SIS Regulation 1862); Article 2 Regulation (EC) No 767/2008 (hereafter, VIS Regulation); Article 1 Regulation (EU) No 603/2013 (hereafter, Eurodac Regulation); Article 1 Regulation (EU) 2017/2226 (hereafter, EES Regulation); Article 4 ETIAS Regulation; Article 2 Regulation (EU) 2019/816 (hereafter, ECRIS-TCN Regulation); Articles 2, 6, 12, 17, 25 Interoperability Regulations 817 and 818; Articles 18 and 87 Frontex Regulation; Article 1 Directive (EU) 2016/681 (hereafter, PNR Directive); Article 6 Council Directive 2004/82/EC (hereafter, API Directive). It must be noted that EU laws and policies related to EU large-scale databases and interoperability have been facing criticism for their clash with certain data protection principles, including purpose limitation. It is uncertain whether such extensive list of purposes will survive the scrutiny of the CJEU in the future.
81. With some differences as to the processing for persons enjoying the right of free movement and third-country nationals, as specified in Article 8(2) and 8(3) SBC.
82. Within Eurosur, processing of personal data other than ship and aircraft identification number is exceptional (Article 89 Frontex Regulation).
83. These categories of personal data are specified in Article 20 SIS Regulations 1861 and 1862, Article 5 VIS Regulation, Article 11 Eurodac Regulation, Articles 17, 18, 19, 20 EES Regulation, Article 17 ETIAS Regulation, Article 5 ECRIS-TCN. Similarly, only certain categories of personal data can be processed/stored in the ESP, Shared BMS, CIR, MID, namely: alphanumeric or biometric data for queries with the ESP (Article 9 Interoperability Regulations 817 and 818), biometric templates for the shared BMS (Article 13 Interoperability Regulations 817 and 818), personal data as from Article 5 VIS Regulation, Article 7 EES Regulation, Article 6 ETIAS Re-

gulation, Article 5 ECRIS-TCN Regulation for the CIR; confirmation files for the MID (Article 25 Interoperability Regulations 817 and 818). Note also that the definition of biometric data in the GDPR, the LED and the EUDPR differs from those contained in border management law. The latter is more restricted, as biometric data encompasses only fingerprints, palmprints, facial images and DNA profiles and not, for example, behavioural characteristics.

84. Annex I PNR Directive and Article 3 API Directive.
85. Brouwer, "Interoperability of Databases and Interstate Trust: A Perilous Combination for Fundamental Rights."
86. See, for example, Article 44 SIS Regulation 1861 and Article 59 SIS Regulation 1862, Articles 24 and 38 VIS Regulation, Article 27 Eurodac Regulation, Article 35 EES Regulation, Article 55 ETIAS Regulation, Article 9 ECRIS-TCN Regulation, Articles 32 and 33 Interoperability Regulations 817 and 818 for the CIR and Article 48 Interoperability Regulations 817 and 818 for the MID.
87. Casiraghi and Calvi, "Biometric Data in the EU (Reformed) Data Protection Framework and Border Management."
88. For instance, border management law requires that: only biometric data of sufficient quality enter the EU large-scale databases (Article 32 SIS Regulation 1861 and Article 42 SIS Regulation 1862, Article 25 Eurodac Regulation); the fingerprint of a third-country national is of sufficient quality when used for automated biometric matching (Article 17 EES Regulation); the facial image of a third-country national is of sufficient quality when used for automated biometric matching (Article 15 EES Regulation); only biometric templates complying with minimum data quality standards are entered in the BMS (Article 13 Interoperability Regulations 817 and 818); performance requirements in terms of the False Positive Identification Rate, False Negative Identification Rate and Failure To Enrol Rate as set in Commission Implementing Acts are complied with (Article 36 EES Regulation).
89. See, for example, Articles 39, 40, 49 SIS Regulation 1861 and Article 53, 54, 55, 64 SIS Regulation 1862, Articles 23 and 25 VIS Regulation, Articles 16 and 18 Eurodac Regulation, Article 34 EES Regulation, Article 54 ETIAS Regulation, Article 8 ECRIS-TCN Regulation, Article 15 Interoperability Regulations 817 and 818 for the Shared BMS, Article 23 Interoperability Regulations 817 and 818 for the CIR, Article 91 Frontex Regulation.
90. See, for example, Article 12 SIS Regulations 1861 and 1862, Article 34 VIS Regulation, Article 28 Eurodac Regulation, Article 46 EES Regulation, Article 69 ETIAS Regulation, Article 31 ECRIS-TCN Regulation, Article 10 Interoperability Regulations 817 and 818 for the ESP, Article 16 Interoperability Regulations 817 and 818 for the Shared BMS, Article 34 Interoperability Regulations 817 and 818 for the CIR, Article 36 Interoperability Regulations 817 and 818 for the MID.
91. See, for example, Article 10 and 16 SIS Regulations 1861 and 1862, Article 32 VIS Regulation, Article 34 Eurodac Regulation, Article 43 EES Regulation, Articles 21, 46, 48 and 59 ETIAS Regulation, Article 19 ECRIS-TCN, Article 11 Interoperability Regulations 817 and 818.
92. See, for example, Articles 4, 9 and 10 SIS Regulations 1861 and 1862, 1.10.3. SIRENE Manual, Article 32 VIS Regulation, Article 3 and 34 Eurodac Regulation, Article 7 and 43 EES Regulation, Article 6 and 59 ETIAS Regulation, Article 19 ECRIS-TCN Regulation, Articles 32 and 33 Interoperability Regulations 817 and 818 for the CIR, Article 42 Interoperability Regulations 817 and 818 for the MID.
93. See Article 12 SIS Regulations 1861 and 1862, Article 34 VIS Regulation, Article 28 Eurodac Regulation, Article 46 EES Regulation, Articles 69 and 70 ETIAS Regulation, Article 31 ECRIS-TCN Regulation; Article 10 Interoperability Regulations 817 and 818 for the ESP, Article 16 Interoperability Regulations 817 and 818 for the Shared BMS, Article 34 Interoperability Regulations 817 and 818 for the CIR, Article 36 Interoperability Regulations 817 and 818 For the MID, Article 89 Frontex Regulation.

94. See, for example, Article 14 SIS Regulations 1861 and 1862, Article 28 VIS Regulation, Recital 19 Eurodac Regulation, Article 38 EES Regulation, Articles 75, 76, 77 ETIAS Regulation, Articles 12, 13 ECRIS-TCN Regulation.
95. See, for example, Article 13 SIS Regulation 1861 and 1862, Article 35 VIS Regulation, Article 36 Eurodac Regulation, Article 47 EES Regulation, Article 61 ETIAS Regulation, Article 21 ECRIS-TCN Regulation.
96. See, for example, Article 11 SIS Regulation 1861 and 1862, Article 26 VIS Regulation, Article 4 Eurodac Regulation, Article 37 EES Regulation, Article 74 ETIAS Regulation, Article 11 ECRIS-TCN Regulation, Article 55 Interoperability Regulations 817 and 818.
97. For instance, in the event(s) of security incidents, Article 45 SIS Regulation 1861 and Article 60 SIS Regulation 1862 require Member States, Europol, Frontex to notify the Commission, eu-LISA, the competent DPA and the EDPS; and eu-LISA to notify the Commission and the EDPS in relation to central system. Article 34 Eurodac Regulation requires Member States to inform eu-LISA and eu-LISA to notify the Commission, Europol and the EDPS in relation to central system. Article 44 EES Regulation requires Member States to notify the Commission, eu-LISA, the competent DPA and the EDPS; and eu-LISA to notify the Commission and the EDPS in relation to central system. Article 60 ETIAS Regulation requires the Member States to notify the Commission, eu-LISA and the EDPS; eu-LISA to notify the Commission and the EDPS in relation to central system; Europol to notify the Commission and the EDPS. Article 43 Interoperability Regulations 817 and 818 requires Member States to notify the Commission, eu-LISA, the competent DPA and the EDPS; eu-LISA to notify the Commission and the EDPS in relation to central system of interoperability components; ETIAS Central Unit and Europol to notify the Commission, eu-LISA, the competent DPA and the EDPS.
98. European Union Agency For Fundamental Rights, European Court of Human Rights, and European Data Protection Supervisor, *Handbook on European Data Protection Law* (Luxembourg: Publications Office of the European Union, 2018), https://doi.org/10.2811/58814.
99. Plixavra Vogiatzoglou et al., "From Theory To Practice: Exercising The Right Of Access Under The Law Enforcement and PNR Directives," *JIPITEC* 11, no. 274 (2020).
100. See, for example, Article 52 SIS Regulation 1861, Article 37 VIS Regulation, Article 47 Interoperability Regulation 817 (for VIS, EES, ETIAS, shared BMS, CIR, MID); Article 29 Eurodac Regulation; Article 64 ETIAS Regulation. Note however that certain authors expressed concerns about the effectiveness of the legal framework at ensuring the exercise of the data subjects' rights, depending, *inter alia*, on its fragmented and complex nature. Diana Dimitrova, "Surveillance at the Borders: travellers and their data protection rights" in *Handbook on Data Protection and Privacy*, eds. Paul De Hert, Rosamunde van Brakel, and Gloria Gonzalez Fuster (Edward Elgar, forthcoming).
101. See, for example, Article 53 SIS Regulation 1861 and Article 67 SIS Regulation 1862, Article 38 VIS, Article 29 Eurodac Regulation, Article 52 EES Regulation, Article 64 ETIAS Regulation, Article 25 ECRIS-TCN Regulation, Article 48 and 49 Interoperability Regulations.
102. Ibid.
103. Ibid.
104. For example, data subjects have the right to request human intervention when using the border control technology (Article 15 SBC); when an automated processing leads to a hit in ETIAS system, the application shall be processed manually by the ETIAS National Unit of the Member State responsible (human in the loop) (Article 26 ETIAS Regulation); when different identities are detected, manual verification is ensured (Article 29 Interoperability Regulations 817 and 818).
105. See, for example, Article 58 SIS Regulation 1861 and 72 SIS Regulation 1862, Article 33 VIS Regulation, Article 37 Eurodac Regulation, Article 45 EES Regulation, Article 63 ETIAS Regulation, Article 20 ECRIS-TCN Regulation, Article 46 Interoperability Regulations 817 and 818.

106. European Union Agency for Fundamental Rights, *Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights*.
107. See, for example, Article 50 SIS Regulation 1861, Article 31 VIS Regulation, Article 35 Eurodac Regulation, Article 41 EES Regulation, Article 65 ETIAS Regulation, Article 18 ECRIS-TCN, Article 50 Interoperability Regulations 817 and 818, Article 89 Frontex Regulation.
108. European Union Agency for Fundamental Rights.
109. For the SIS, national competent authorities responsible for the identification of third-country nationals for the purposes listed in Article 34 SIS Regulation 1861; national competent authorities for the purposes listed in Art. 44 SIS Regulation 1862; national competent authorities responsible for naturalisation for examining an application of naturalisation (Article 34 SIS Regulation 1861 and Art. 44 SIS Regulation 1862); vehicle registration services, boat and aircraft registration services, firearms registration services as specified in Articles 45, 46 and 47 Regulation 1862. Links between alerts do not affect the right to access (Article 48 SIS Regulation 1861). For the VIS, duly authorised staff of the visa authorities as specified in Article 6 VIS Regulation. For the Eurodac, for law enforcement purposes, as specified in Article 6 Eurodac Regulation. For the EES, duly authorised staff of the national authorities of each Member State as specified in Article 9 EES Regulation. For the ETIAS, duly authorised staff of the ETIAS Central Unit and of the ETIAS National Units as specified in Article 9 ETIAS Regulation. For the ECRIS-TCN, only duly authorised staff have access to the data for the performance of their tasks as specified in Article 13 ECRIS-TCN Regulation. For the ESP, see Article 7 Interoperability Regulations 817 and 818. For the CIR, see Articles 18 and 20 Interoperability Regulations 817 and 818. For the MID, see Article 26 Interoperability Regulations 817 and 818. Note however that certain authors criticised the rules on the functionality of the MID, considered ambiguous, *inter alia*, in relation to the access of the SIRENE Bureaux to the links. Diana Dimitrova and Teresa Quintel, "Technological Experimentation Without Adequate Safeguards? Interoperable EU Databases and Access to the Multiple Identity Detector by SIRENE Bureaux."
110. For access by Europol to the SIS, see Article 35 Regulations 1861 and Article 48 SIS Regulation 1862; to the VIS, see Article 3 VIS Regulation; to the Eurodac, see Article 21 Eurodac Regulation; to the EES, see Article 33 EES Regulation; to the ETIAS, see Article 53 ETIAS Regulation; to the ECRIS-TCN, see Article 14 ECRIS-TCN Regulation; to the ESP, see Article 7 Interoperability Regulations 817 and 818; to the CIR, see Article 17 Interoperability Regulations 817 and 818. For access by Eurojust to the SIS, see Article 49 SIS Regulation 1862; to the ECRIS-TCN, see Article 14 ECRIS-TCN Regulation. For access by Frontex to the SIS, see Article 36 Regulations 1861 and Article 50 SIS Regulation 1862.
111. See, for example, Article 5 Interoperability Regulations 817 and 818, Article 14 ETIAS Regulation, Recital 13 Eurodac Regulation.
112. See, for example, Article 5 Interoperability Regulations 817 and 818, Article 14 ETIAS Regulation.
113. See, for example, Article 37 EES Regulation.
114. Ibid.
115. See, for example, Article 5 SBC.
116. See, for example, Article 34 SBC.
117. See, for example, Articles 8a and 8b SBC.
118. Ibid.
119. See Regulation (EC) No. 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items (Dual-use Regulation).
120. See, for example, Article 67 TFEU.
121. See, for example, Article 8c SBC, Article 5 Interoperability Regulations 817 and 818, Article 14 ETIAS Regulation.
122. See, for example, Article 3 Eurodac Regulation.

123. See, for example, Article 7 SBC, Article 14 ETIAS Regulation, Article 5 Interoperability Regulations 817 and 818.
124. See, for example, Article 8c SBC.
125. See, for example, Article 17 EES Regulation, Article 9 Eurodac Regulation.
126. See, for example, Articles 32 and 55 SIS Regulation 1862.
127. Ibid.
128. See, for example, Article 20 Interoperability Regulation 818.
129. See, for example, Article 32 SIS Regulation 1862.
130. See, for example, Article 55 SIS Regulation 1862.
131. See, for example, Article 16 SBC.
132. See, for example, Article 4 SBC.
133. See, for example, Article 5 Interoperability Regulations 817 and 818.