WRITTEN BY:
Romain Lanneau

DATA PROTECTION HANDBOOK ON ASYLUM AND MIGRATION IN EUROPE

OCT 2025
STATEWATCH

Publication information

Author: Romain Lanneau

Editor: Chris Jones

Design & layout: McKensie Marie

Thanks to Lori Roussey, *Data Rights*.

Published by Statewatch, October 2025.

This report was produced as part of the project 'Data exchange, exclusion and denial at the borders: Upholding the right to an effective remedy', supported by ***Privacy International***.

About Statewatch

Statewatch produces and promotes critical research, policy analysis and investigative journalism to inform debates, movements and campaigns for civil liberties, human rights and democratic standards.

statewatch.org
+44 (0) 7836 296 043
MayDay Rooms, 88 Fleet Street, London EC4Y 1DH,UK

Support our work

Support our work to expose state power and inform dissent by making a donation. And join our mailing list to stay informed and help spread ourwork.

Scan the QR code above or visit:

— **Donation page**

— **Mailing list sign-up**

Registered UK charity number: 1154784

Registered UK company number: 08480724

Registered company name: The Libertarian Research & Education Trust

Registered office: 88 Fleet Street, London EC4Y 1DH, UK.

Contents

Introduction 9

1. The 'datafication' of immigration and asylum 11

1.1. Context and background 12
1.2. Digital technologies in immigration and asylum proceedings 17

2. Data protection and privacy law: background and basics 31

2.1. Defining privacy 32
2.2. Data protection as a fundamental right 34
2.3. Data protection: definitions and key principles 37
2.4. Data protection principles 45
2.5. Applicable law 52
2.6. The proportionality principle 54

3. Opportunities for redress 63

3.1. The right of redress 64
3.2. Restrictions 70
3.3. Automated decision-making 72
3.4. From access to redress 75

Endnotes 83

Glossary

access to documents

The principle of access to documents is a fundamental right, set out in article 42 of the EU Charter of Fundamental Rights. Regulation (EU) 1049/2001 governs the ways people and entities (often, but not always, EU citizens or EU-registered) can request access to documents held by EU institutions, agencies and bodies.

algorithm

A process designed to solve a specific problem, whether qualitative, quantitative, or a mixture of the two. In common use it refers to programming instructions for computer software. Algorithms can be used to score people's credit worthiness, whether they should be granted a visa, and countless other things.

biometric data

Data created from biometrics. Biometrics are measurements and calculations related to human characteristics and features. Images of fingerprints, photographs, voice recordings, and even recordings of a person's gait may be considered biometric data, amongst other things.

Common Identity Repository (CIR)

A large-scale EU database for storing identity data (biographic and biometric details) on non-EU citizens.

Convention 108

The 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

data protection

Legislation, policies, practices and processes for protecting personal data from unauthorised collection, use, access or disclosure.

data protection authority

A national public authority responsible for monitoring the application of data protection law. At EU level, the equivalent is the European Data Protection Supervisor. Also referred to as a supervisory authority.

data protection impact assessment (DPIA)

A process designed to help individuals and organisations comply with data protection law by analysing, identifying and minimising the data protection risks of a project or plan.

data subject

An identified or identifiable natural person about whom personal data is processed.

Entry/Exit System (EES)

A large-scale EU database designed to record the times and locations at which non-EU citizens enter or exit the Schengen area, by collecting and checking biometric and biographic data.

EU agencies

Bodies set up by the EU to carry out particular tasks or functions. In this handbook, it refers to agencies operating in the field of justice and home affairs, in particular the European Border and Coast Guard Agency (Frontex), the European Agency for Law Enforcement Cooperation (Europol), and the European Asylum Agency (EUAA).

Eurodac

A large-scale EU database used for storing and comparing fingerprints, photos and other data on asylum seekers and irregular migrants in the EU and some associated countries.

European Criminal Records Information System for Third Country Nationals (ECRIS-TCN)

A large-scale EU database for member state authorities to check whether a non-EU citizen has a criminal record in another member state.

European Data Protection Board (EDPB)

The advisory body that brings together the national data protection authority of each EU member state.

European Data Protection Supervisor (EDPS)

The EU body responsible for monitoring the application of data protection law by EU institutions, agencies and bodies. At national level, the equivalent is the data protection authority. Also referred to as a supervisory authority.

European Travel Information and Authorisation System (ETIAS)

A large-scale EU database for storing applications from non-EU citizens for travel authorisations, which give permission to travel to the EU. An automated profiling system is used to assess all applications.

freedom of information

The right of individuals to access information held by public authorities. EU member state governments tend to have freedom of information laws; the equivalent in the EU is access to documents legislation.

General Data Protection Regulation (GDPR)

An EU law passed in 2016 on the protection of personal data. It is the default law to be applied in the migration and asylum context.

Interoperability

The ability of different electronic information systems and databases to ‘talk’ to one another.

Law Enforcement Directive (LED)

An EU law passed in 2016 on the protection of personal data in national law enforcement contexts.

personal data

Information relating to an identified or identifiable natural person.

processing of personal data

Any operation or set of operations performed on personal data, whether or not by automated means. It encompasses collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Regulation on data protection in EU institutions, agencies and bodies

An EU law passed in 2018 on the protection of personal data in EU institutions, agencies and bodies.

Schengen Information System (SIS)

A large-scale EU database that enables the sharing of personal and other data between national and EU authorities for the purposes of law enforcement, criminal justice, immigration enforcement and border control.

sensitive data/special categories of personal data

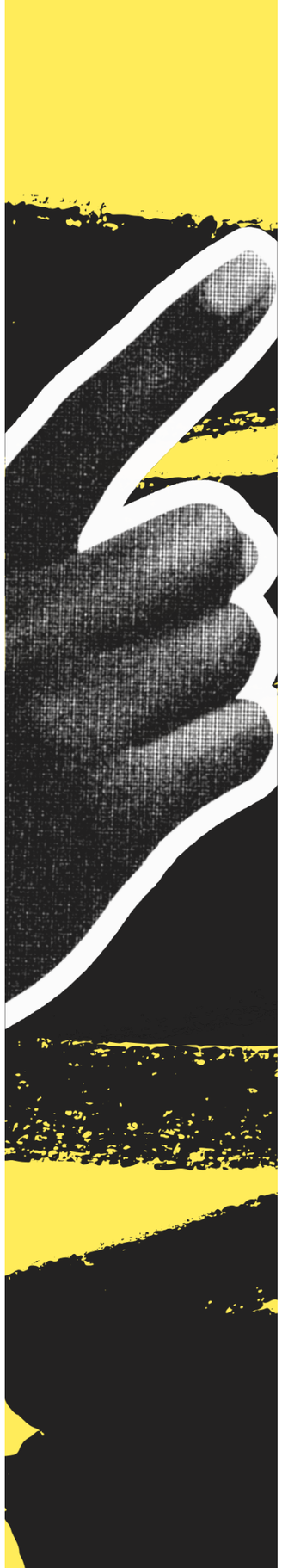
Categories of personal data which merit higher protection due to their sensitivity and potential to cause harm, such as political opinions or health data.

supervisory authority

A data protection authority.

Visa Information System (VIS)

A large-scale EU database used to store information on applicants for visas to the Schengen area. An automated profiling system to assess all applications is being introduced.



Introduction

The EU's immigration and asylum system is governed by a complex set of rules. As well as being regularly amended by legislators, those rules are also subject to frequent interpretation (and re-interpretation) by the courts.

The increasing use of digital technologies and databases for the enforcement of immigration and asylum law adds a further twist to this complicated scenario. Personal data gathered, stored and processed by the authorities may be crucial in the assessment of an individual's claim for international protection, for a visa, or to contest deportation.

Understanding these systems and technologies, and the laws that govern them, is therefore increasingly important for immigration and asylum practitioners. Such an understanding needs to be underpinned by knowledge of privacy and data protection rights, and the policies, legislation, practice and jurisprudence that shape them. This handbook is designed to offer the foundation of that understanding.

Section 1 provides the context for the growing deployment of digital technologies as part of EU immigration and policy. Borders and the people who cross them are often treated as testing grounds for new technologies, the development of which is increasingly outsourced to private companies by public authorities. An overview of some key technologies used at both EU and national level is offered.

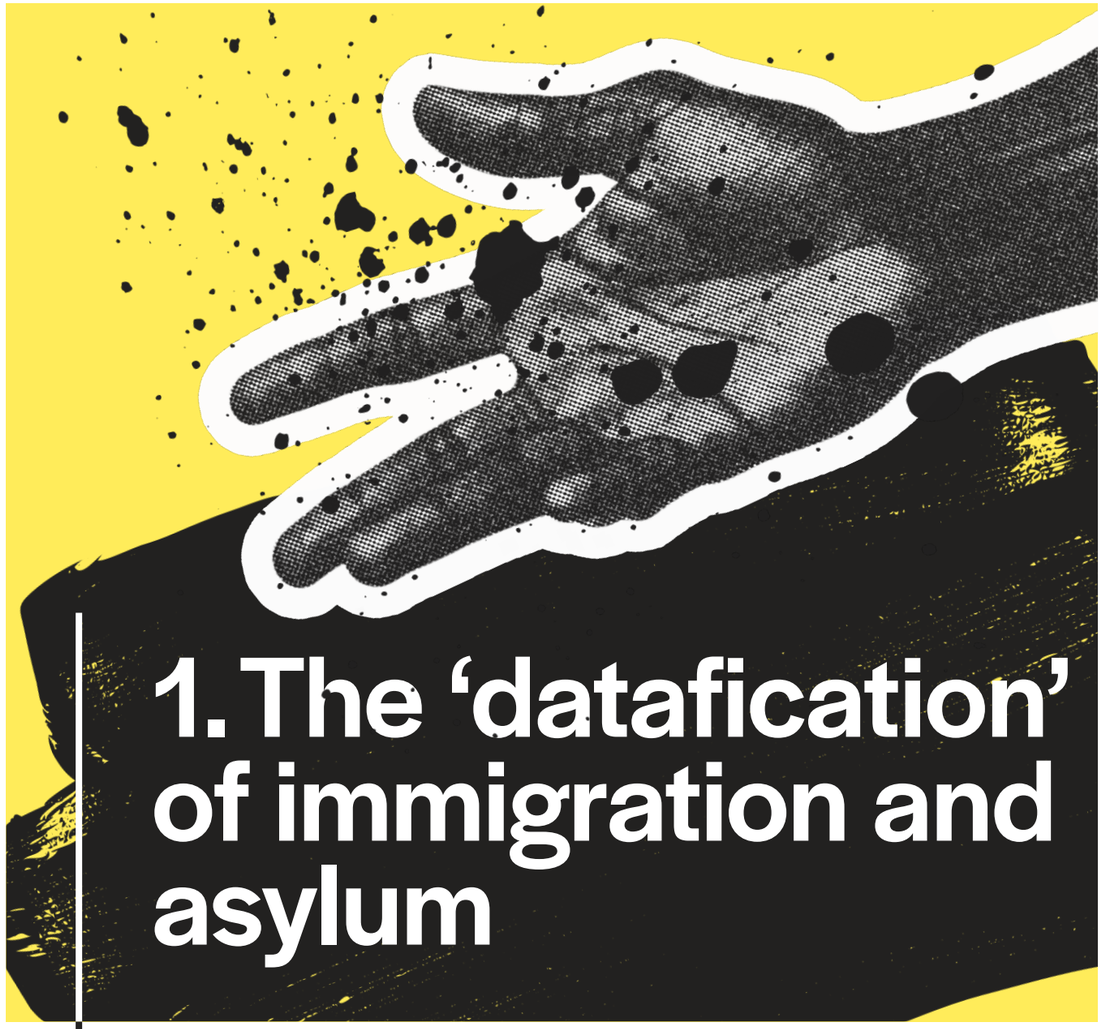
Section 2 gives in-depth but accessible explanations of key privacy and data protection principles, terms and

concepts. It provides an overview of the six data protection principles, explains relevant EU data protection legislation, and looks at how courts have interpreted questions related to privacy and data protection, including in the context of immigration and asylum cases.

Section 3 examines how data protection law can be used to seek redress for individuals. It explains the different components of an individual's right to access their own personal data, and to have it rectified or deleted if needs be. It then explains how to exercise the right of access, and the different bodies from whom redress can be sought.

Given the dire situation for many people in the immigration and asylum system(s) in the EU, the issue of data protection may seem relatively minor. However, infringements of privacy and data protection rights can underpin other rights violations. Think, for example, of a deportation based on mistaken identity, refusal of a visa due to an algorithmic assessment, or continued harassment from the police due to being mislabelled a danger to national security.

The avenues for redress offered by data protection law can offer ways to help seek justice in these and many other situations. As increasing amounts of personal data are gathered from people crossing borders, understanding data protection law and its uses will only become more important. We hope this guide is useful for people seeking justice in the EU's immigration and asylum system, and for the lawyers, case workers, volunteers and others who support them.



1. The 'datafication' of immigration and asylum

Whether people arrive in Europe in a 'regular' or 'irregular' manner, their journeys - and their experiences upon arrival - will be mediated by digital technologies that are used to store and process their personal data.

The use of personal data in the EU's border, immigration and asylum regimes has intensified over the last decade. Understanding this 'dataficiation' makes clear why data protection law is a crucial tool for immigration and asylum practitioners.

This section examines the context and background of the situation, before looking at the personal data and digital technologies that can be used in immigration and asylum proceedings.

1.1. Context and background

Digital technologies used to process personal data have become increasingly central to the EU's immigration, asylum and border policies since the 1990s. This trend will continue in the years to come, as more information is digitised and new ways of processing and sharing it are introduced.

These trends have been shaped by a number of themes, three of which will be briefly examined below: the use of 'experimental' technologies on non-citizens, the role of the private sector, and the growing powers of EU agencies.

1.1.1. Experimental technologies

In a 2020 report, researcher Petra Molnar argued that:

> *Certain places serve as testing grounds for new technologies, and these places are usually where regulation is limited and where an 'anything goes' frontier attitude informs the development and deployment of surveillance at the expense of humanity.*[1]

Her research shows that European borders are one of those places. However, the idea that invasive experiments can be tested on vulnerable people is certainly not unique to Europe.

Antony Loewenstein has analysed how Israel uses military-grade surveillance technologies in the occupied Palestinian territory, before advertising those technologies as "battle-tested" at arms fairs around the world.[2] European states have proven loyal customers, paying those companies to help them fortify borders,[3] spy on migrant rights defenders[4] and conduct drone surveillance of the Mediterranean.[5]

The unpleasant origins of many modern-day surveillance technologies can be traced even further back in time. Chloé Berthélémy and Laurence Meyer note:

> *It's no surprise that biometrics are becoming the centrepiece of states' expanding technological surveillance systems and, it's even less surprising, that they're a part of migration control policies. The very origin of biometric surveillance stems from colonial practices of dominating and discriminating against certain groups of people.*[6]

Once a technology has proven its worth for identifying, tracking or monitoring non-citizens, it may be applied to citizens as well. In 2003, EU states began systematically fingerprinting asylum-seekers. A year later, a new law was introduced that made it mandatory to include fingerprints in almost all EU citizens' passports.[7] In 2019, the same requirement was introduced for national identity cards, hot on the heels of laws setting up huge new biometric databases targeting non-citizens.[8]

1.1.2. Private interests

Since at least 2008, EU states have introduced severe austerity measures, cutting funding for a vast array of public services. As part of the same policy programme, private actors have been given responsibilities previously held by public institutions. This has undermined social services and has been used by politicians and media outlets to exacerbate tensions over certain categories of people – often, non-citizens – receiving state support.

The immigration and asylum sectors are no exception, though the degree to which privatisation and outsourcing has taken place differs from state to state.[9] The increasing demand for digital 'solutions' to policy questions has also facilitated a growing role for the private sector.

In the EU this can be seen prominently in the huge contracts awarded for border surveillance, database construction and management, or the construction and operation of camps and detention centres. Generous EU budgets have supported these developments.[10]

Private actors have a vested financial interest in the continuation or introduction of policies that will increase their profits. Their growing role in immigration and asylum policy implementation also has other effects – for example, regarding transparency.

Right to information legislation grants people the right to ask public bodies for information they hold or should hold. EU institutions, agencies and bodies are bound by a 2001 law on access to documents.[11] Many EU member states have freedom of information laws covering public sector institutions.[12]

Private actors, on the contrary, are not bound by any such principles. Information on the role of private actors might be accessible through requests to public authorities for information on contracts, or on communications between public authorities and private companies. However, transparency laws usually contain exceptions that make such information difficult to access.

The *Border Violence Monitoring Network* has condemned the fact that their requests on border surveillance technologies and projects "were often rejected on the grounds of security or commercial interest, despite [the technologies and projects] being publicly funded."[13] This means it is often impossible to obtain information on a technology's invasiveness or effectiveness.

Patrick Breyer, a former MEP, knows this all too well. He was denied access to documents produced by a highly-controversial project that aimed to develop an automated lie detector for use at border crossings.[14] He took the case all the way to the Court of Justice of the EU. Judges ultimately ruled that the commercial interests of the consortium participants, including private companies and public academic institutions, prevailed over the need for transparency, despite ethical concerns over the development of the technology.[15]

1.1.3. EU agencies

The academic Lilian Tsourdi argues that, since 2019, EU agencies have been at "the forefront of [EU] policy implementation."[16] This is

particularly the case in the fields of immigration and asylum: the roles, budgets and staffing of Frontex, the EU Asylum Agency and Europol have been substantially increased by legislators.[17]

The mandates of these agencies were initially focused on "information exchange, training and risk analysis," notes Tsourdi. Extensions to those mandates have added new roles including joint policy implementation, "operational support and administrative cooperation," as well as "functions which have the potential of steering policy implementation."[18] Democratic scrutiny and control of their operations, however, remains limited.

Agencies' tasks include the gathering and exchange of personal data. Frontex officials, for example, carry out "debriefing" interviews with people who have just crossed borders. The aim is to gather information on potential smuggling routes, which is shared with Europol, the EU's policing agency. The practice was condemned as illegal by the European Data Protection Supervisor (the EU's data protection authority), though it continues in a more limited fashion.[19]

European agencies also have a role guiding research into, and developing, new technologies.[20] Given the findings of the European Data Protection Supervisor (EDPS), it would be reasonable to wonder whether algorithms have been trained and tested on unlawfully processed personal data.[21]

A culture of secrecy is one obstacle to detailed knowledge about the growing roles of these agencies. For example, three investigative journalists have denounced the fact that "Europol routinely obstructs access to key documents through procedural delays, heavy redactions, or blanket rejections on "public security" grounds."[22] Frontex has sought thousands of euros in legal costs from people taking it to court in transparency cases, ignoring a longstanding practice of EU institutions not to do so.[23]

1.1.4. How technology 'works'

This official opacity cannot always be maintained when those technologies are deployed. Some are clearly, deliberately visible.

Think, for example, of border fences topped with razor wire and punctuated by surveillance cameras, or armed border guards carrying tablet computers.

These offer "a visual demonstration of commitment to EU border security,"[24] a function that may be more important than their role in preventing irregular migration. As EU agencies themselves have remarked, demand for migrant smuggling services is driven by people's "need to bypass reinforced borders several times."[25] It is governments, states and corporations that are 'reinforcing' those borders, whilst claiming to crack down on migrant smuggling.

The visibility of certain technologies also makes it possible to name things as they are. As one person living in the 'Closed Controlled Access Centre' on the Greek island of Samos said when asked about the camp's surveillance cameras: "I don't believe this is a refugee camp... this is not a camp. This is prison... How come in a camp there are so many cameras?"[26]

Technologies deployed to enforce immigration and asylum policy therefore, do not necessarily need to 'work' as advertised. In some cases, the fact that they are visible and contribute to a hostile environment towards people on the move is enough. This argument has also been made with regard to state databases, by the academic Elisabeth Badenhoop:

> *...the primary function of migration databases seems to be a symbolic one, that is (re)producing the image, belief, and authority of the modern state as capable of exercising migration control, both to an internal and external audience.*[27]

Whether or not the digital technologies deployed to enforce asylum and immigration policies can ever provide the control states are seeking, they have real effects on the people subjected to those policies. Examining some of those technologies in more detail makes clear how.

1.2. Digital technologies in immigration and asylum proceedings

Within the context outlined above, a diverse array of digital technologies are being developed, tested and used. The academic Derya Özkul has undertaken an encyclopaedic mapping of technologies deployed for immigration and asylum policies in the EU.[28] She looks at those technologies geographically:

— those used prior to arrival;

— those used at the border; and

— those used within EU territory.

This section draws on Özkul's work to examine technologies that can have a direct impact on individual cases and decisions in asylum and immigration proceedings. It does not examine, for example, border surveillance systems such as drones.

The technologies below can be considered as dealing with either the **identification** of individuals, **monitoring** their location, and/or supporting the **assessment** of their case.

1.2.1. Algorithmic video surveillance

Purpose: monitoring

La Quadrature du Net, a French civil society organization researching the impact of digital technologies on fundamental rights, has documented the development and increased reliance of public authorities on algorithmic video surveillance. They define the practice as:

> *A software used by the police that analyzes images from video surveillance cameras. This software is designed to detect, identify, or classify specific behaviors, situations, objects, or people.*[29]

The deployment of algorithmic video surveillance has been justified on the basis of the exceptional security risk presented by mass events. In 2023, in the name of preventing terrorism, the French government introduced emergency legislation to authorise the use of algorithmic video surveillance during the 2024 Olympic games.

The move was denounced by legal scholars and *La Quadrature du Net* as a power grab to normalise society-wide state algorithmic surveillance.[30] A year after the event, despite no further proof of its usefulness, the French government decided to continue the experiment.[31]

These technologies are being used across Europe. In the Samos detention camp in Greece, the organisations *I Have Rights* and *Homo Digitalis* reported that the Greek state has set up an algorithm-assisted surveillance camera network that supposedly identifies in real time when a person's behaviour is dangerous.[32] Every person working or living in the camp is monitored by video surveillance.

The system has been successfully challenged before the Greek data protection authority, and is analysed in more detail in section 2. But, so far, the cameras have not been shut down. Far from it – more appear to have been deployed, at Greece's borders with Turkey and Bulgaria.[33]

1.2.2. Automated visa and travel authorisation assessments

Purpose: assessment

As of 2026, every non-citizen travelling into the Schengen area will require some form of permission to travel – either a visa or a travel authorisation. Like visa applicants, travel authorisation applicants will have to answer a series of questions about their employment, education, and so on – invasive, though certainly less so than applying for a visa. Travel companies (for example, airlines or coach companies) will be required to check a person's permission to travel.[34]

Permission (or denial) will be granted by EU and member state authorities, aided by algorithmic profiling and assessment tools.

Those tools will be hosted by Frontex as part of the European Travel Information and Authorisation System (ETIAS) and the Visa Information System (VIS).

Algorithmic assessment tools have themselves been assessed by the Court of Justice of the EU. The court imposed some limits on their use, in a judgement concerning the EU's Passenger Name Record (PNR) Directive.[35] The law requires that airline companies provide to police forces data on air passengers travelling into the EU, for the purpose of seeking out criminals. Algorithmic tools are used for this purpose.

The CJEU has firmly prohibited "self-learning systems ('machine learning'), capable of modifying without human intervention or review the assessment process," especially if deployed to decide who is a risk and how this should be weighted with other concerns, such as individual rights.[36] In the visa and travel authorisation context, the final decision on a refusal has to be made by a human. However, it remains to be seen to what extent officials will deviate from the assessments produced by computers.

1.2.3. Biometric data

Purpose: identification

Biometric data is defined as:

> *Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [fingerprint] data.*[37]

Biometric data has become key to modern identification systems, even creeping into consumer devices. Think, for example, of unlocking a smartphone using your face or fingerprint.

In the immigration context, the first large-scale EU tool to make use of biometric data was the **Schengen Information System (SIS)**. It

was set up as a "compensatory" measure for the opening of internal borders within the Schengen area. Governments agreed that freedom of movement within the area required stronger control over external borders, and the identification of undesirable people within the territory.

Every Schengen member state can create 'alerts' in the SIS on individuals who should be questioned, arrested or refused entry. Alerts can also be created on objects, for example stolen vehicles or missing identity documents. Officials such as border guards and police officers can then search the database for those alerts.

Alerts on persons to be refused entry to the Schengen area (a category originally named "unwanted aliens"[38]) have consistently been the most numerous type of alerts on persons.[39] They can include a wide variety of data, including fingerprints and, following the most recent reform, photographs. DNA and palm prints can also be included in certain cases.[40]

In the asylum context, the first large-scale biometric system in the EU was **Eurodac**,[41] which was set up to help enforce the Dublin agreement. The Dublin Agreement introduced the 'first country' rule into EU asylum law. Asylum-seekers' fingerprints are collected and stored in a centralised database, accessible to all asylum authorities in Europe. If someone registered in the database travels to another EU member state and claims asylum, they are (absent any mitigating circumstances[42]) sent back to the country where they had first registered a claim.

Eurodac was first discussed by EU governments in 1994, and began operating in 2003.[43] In 2024 new legislation governing the system was approved by EU legislators. It lowers the age limit for data collection from 14 to six years of age.[44] In the year 2000, the European Parliament considered that "the threshold of 14 is contrary to the existing international instruments on children's rights."[45]

The 2024 law also massively expands the categories of person whose data will be registered in the system. Rather than solely enforcing the Dublin system, Eurodac will now also be used for registering undocumented migrants, with a view to aiding their deportation.[46]

Biometrics are central to the majority of the EU's large-scale information systems, as detailed in Box 1. While these immense databases were originally designed as separate systems, operating as 'silos', the data they hold is now being interconnected. The aim is to facilitate the identification of individuals, and to make new uses of the personal data that was previously stored separately, for discrete purposes.

LARGE-SCALE EU INFORMATION SYSTEMS

The academic Niovi Vavoula charts the evolution of the EU's large-scale databases and information systems through three phases.

Phase I: 1990s-2001

In this phase, the Schengen Information System was launched and Eurodac was put into development. At the time, keeping separate databases was advertised as guarantee for the security of the systems, and as a way to protect individual rights.[47]

Phase II: 2001-2010s

The terrorist attacks in the USA on 11 September 2001, and attacks in Spain (2003) and the UK (2005) transformed political debates on borders, asylum, immigration and security. Every foreigner entering the territory was considered a security risk to be controlled and monitored.[48]

During this period the **Visa Information System (VIS)** was set up. The VIS stores information on all Schengen visa applicants, including their fingerprints and photograph. For short-stay visas, it is used to keep track of people whose applications are successful, and those whose applications were not.

During this period **Eurodac** and the **SIS** were also expanded. A reform of Eurodac added, in 2015,[49] a new category of persons to the database: "Third country nationals or stateless persons apprehended in connection with the irregular crossing of an external border."[50] This shifted the system from its original purpose (determining the state responsible for an asylum claim), introducing an element of control over irregular migrants.

The SIS was also expanded, undergoing its transformation, according to Vavoula: "from a mere reporting mechanism to a general investigation tool."[51] The second-generation Schengen Information System (SIS II) was proposed in 2005 by the Commission and adopted in 2007.[52] It gave access to SIS data to security and intelligence services, Europol and national judicial authorities responsible for investigating and prosecuting crime.[53]

During this period the EU also underwent a major expansion, with new member states joining in 2004 and 2007. The authorities in those states were obliged to set up their own databases and connect them to the central systems hosted in Strasbourg.

Phase III: 2010s-present

During this phase, legislation has been approved for a range of new information systems, which are about to come into use or currently under construction. Data collection requirements have also been expanded. These additions are meant to ensure that any third-country national present in EU territory (and many who have attempted to enter EU territory) will be inscribed in digital databases for screening, identification and monitoring purposes.

The **Entry/Exit System (EES)**, adopted in 2017,[54] will cover all short-stay visa holders and visa-exempted travellers. Registrants must provide biometric and biographic information, used to automatically calculate the length of time an individual is permitted to stay (and has stayed) in the Schengen area. This automatic detection of 'overstayers' is supposed to aid in the enforcement of immigration legislation.

The **European Travel Information and Authorisation System (ETIAS)**, adopted in 2018, will assist in the granting of travel authorisation for all visa-exempt nationals,

including by giving an automated recommendation on security or health risk.[55] Unlike the other systems examined here, ETIAS will not store biometric data, but applications will be cross-referenced with biometrics and biographic data from the EES. ETIAS therefore relies upon the processing of sensitive personal data.

Finally, there is the **European Criminal Records Information System for Third Country Nationals (ECRIS-TCN)**, adopted in 2019.[56] This provides for the electronic exchange of non-citizens' criminal record information between member states.

The biggest change in Europe's digital border has been the adoption of the **interoperability** rules in 2019. Databases are being made "interoperable" to connect previously separated data and enable seamless search across the systems. For example, if you apply for a visa and you have a criminal record in an EU member state, interoperability between the VIS and the ECRIS-TCN means the criminal record should be taken into account in an assessment of the visa application.

The interoperability rules mandate the creation of four other large-scale information systems, the most notable of which is the **Common Identity Repository (CIR)**.[57] This will be used to store "identity data" (biometrics and biographic information) from the systems examined above, to facilitate the searching and cross-referencing of different databases. It will, initially, be able to store records on up to 300 million people.

A separate, specialised policy area

Over the last three decades, the EU has created an infrastructural behemoth to monitor and control the movement of migrants. These long and complex laws have, according to Vavoula, "become a policy field in their own right."[58]

An article by the academic Julien Jeandesboz explains how the legislative process for these systems involves highly technical issues that are examined by the same experts over the years. This makes the overall process an exclusive discussion that is barely-comprehensible to anyone else.[59]

Last year, the EU Fundamental Rights Agency (FRA) produced an information platform that provides information about the legal basis and functioning of the systems. It also offers advice on how to support people whose rights may have been violated.[60]

1.2.4.

1.2.5. Dialect recognition

Purpose: identification, assessment

Dialect recognition technologies have, so far, been used to aid in assessing the nationality of a person during the asylum procedure.[61] For example, someone with no identity documents, or false identity documents, may have their dialect analysed with the aim of determining their country of origin.

Germany began using a tool for dialect recognition as early as 2017. A speech sample is collected from the asylum applicant, and processed by software that has been trained on speech recordings of people from a range of countries.[62] The software compares the sample with the training data and suggests a potential country of origin. The result is included in the person's asylum application file.

The ability of the tool to accurately determine someone's country of origin has been debated by linguists. The tool is based on an assumption that language can be encoded by feeding a sample of representative data. However, Lutz Rzeha, a linguist at the University of Berlin, has argued that language "changes constantly," and that technology is unable to adapt to this reality.[63]

Nevertheless, an EU-wide tool is on the way. The Dutch authorities have taken the lead on its development, which is supposed to be finalized in 2027. The results of the project will then inform European practice. The academic Cecilia Manzotti has warned that the automated software could affect the perceived credibility of asylum seekers' claims, while offering them no realistic means of redress.[64]

1.2.6. GPS tagging

Purpose: monitoring, assessment

In Europe, the practice of putting GPS (Global Positioning System) tags on people in immigration proceedings began in the UK.[65] Satellites can then be used to track that person's location. Since 2022, remote electronic monitoring has been a required condition of immigration bail in England and Wales for most people facing deportation.

GPS tags provide minute-by-minute information on the wearer's location. The practice has been presented as an alternative to detention, but it has strict obligations that severely limit the movement of a person. Some critics argue that it amounts to *de facto* detention,[66] and individuals subjected to tagging have described it as a "type of torture."[67] A report produced for the Home Office, after a successful legal challenge against the program, concluded that the GPS tagging of asylum seekers was ineffective.[68]

In March 2025, the European Commission published a proposal for a new deportation law. The proposal includes measures on alternatives to detention that would allow member states to use "electronic monitoring."[69] The law, if approved in this form, could provide a legal basis for GPS tagging, or other forms of remote electronic monitoring, in all EU member states.

Litigation relating to these practices is examined in more detail in section 2.

1.2.7. Mobile biometric identification devices

Purpose: identification

Police and immigration officials make increasing use of mobile biometric identification devices. These make it possible to scan fingerprints or faces in the street (or anywhere else) to verify or establish an individual's identity.[70] They are likely to be used in conjunction with national databases and the EU's large-scale biometric databases.

Checking an individual's fingerprint or face through a mobile device would make it possible to see, for example, whether someone holds a Schengen visa, is registered in Eurodac as an asylum applicant, or is not registered in a database at all – implying that they are in an irregular situation.[71]

These technologies are being used by agencies with dismal track records of racism. Ethnic profiling is illegal. It is also widespread amongst police forces and other authorities – for example, at the border.[72] As one police officer cited in a 2025 *Statewatch* report said: "I do use ethnic profiling, but I don't know how I should do my job differently. We've got to discriminate because otherwise, we wouldn't catch anyone."[73] A 2022 *Statewatch* report warned:

> *With authorities seeking to increase the number of deportations, and skin colour treated as a proxy for an individual's immigration status, any attempt to increase the number of identity checks has serious implications for ethnic minority EU and non-EU citizens alike.*[74]

At the time the report was published, there was evidence that the authorities in Denmark, France, Germany, Greece, the Netherlands, Spain and Sweden, as well as in the UK, were using or seeking to acquire mobile biometric identification devices of one form or another.[75]

1.2.8. Mobile phone data analysis

Purpose: identification, assessment

As far back as 2017,[76] authorities in the EU have been seizing phones from migrants and asylum-seekers in order to extract and analyse the data they hold. This practice, sometimes carried out with dedicated hardware and software,[77] is supposed to help both identify individuals and assess their asylum claims or immigration applications. Activists also say that the French police, trying to identify smugglers, analyse mobile phones seized from migrants who have crossed the border with Italy.

Practices differ across Europe. In some cases, the consent of the person is requested before authorities can access the phone. Analysis may also be limited to a certain subset of information stored in the phone. In this scenario, case workers are granted access to information deemed relevant for detecting possible contradictions with regard to an individual's claimed identity or country of origin.

But, in the Netherlands, for example, "extraction is not limited and can be done in all cases." In Denmark, the immigration service can ask asylum applicants to share their Facebook profiles.[78] This practice has also been reported in Italy when examining the age of unaccompanied children.[79] These practices give access to a plethora of highly sensitive personal data that can easily be abused.

Litigation relating to these practices is examined in more detail in chapter 2.

1.2.9. Conclusion: Technologies for the state

The diverse technologies deployed to enforce EU immigration and asylum policies are, according to Derya Özkul:

> *...designed to benefit state authorities. Migrants' (asylum seekers' and refugees') interests and voices have generally not been included in the design and the decision to employ many of them.*

New identification technologies will make it easier for the authorities to track and control people's movements, and will exacerbate the longstanding problem of ethnic profiling.

To prove their identity or have an asylum claim assessed, people may be asked – or require – to give access to their phone, granting the authorities access to highly sensitive personal data.

GPS tagging is presented as an alternative to detention, but it imposes geographical constraints on a person's movement and generates highly intrusive personal data on already disadvantaged populations, whilst subjecting them to severe mental distress.

Officials claim that automated assessment tools can support more accurate decision-making, but they may wrongly suggest that an individual is a potential risk to national security.

No matter what these tools are for or how they are used, they are all reliant to some degree on personal data. This is why knowledge of data protection law is so vital for immigration and asylum practitioners.

2. Data protection and privacy law: background and basics

The understanding and interpretation of the right to privacy in Europe has evolved significantly over the last five decades.

The right to data protection, generally seen as part of privacy, was not recognised as a separate fundamental right until much more recently.

Their application in the migration and asylum context has seen European courts attempt to strike a balance between the rights of individuals and the interests of states.

2.1. Defining privacy

Privacy does not have a consistent definition worldwide.[80] In the 1970s, the development of computerised information systems, in particular by states, led to discussions on the need for a new understanding of the right to privacy. A political backlash against state surveillance and the use of new technologies saw a push for regulation on the right to privacy and the emergence of the right to data protection.[81]

In Europe, several countries introduced legislation, amendments to their constitutions and high courts issued jurisprudence.[82] **In 1981, the first legally-binding international instrument on data protection and privacy was adopted**: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, often referred to as Convention 108.

The convention was drafted by the Council of Europe, an international organisation that promotes human rights, democracy and the rule of law in Europe. It established the European Convention on Human Rights (ECHR) and ensures the Convention is enforced through the European Court of Human Rights (ECtHR).

The ECtHR has interpreted the right to privacy in its jurisprudence on **article 8 of the Convention, the right to respect for private and family life**. This interpretation of article 8 was drawn up in 1967, when the Consultative Assembly of the Council of Europe decided to respond to the spread of technological devices and interferences with the right to privacy.

The Consultative Assembly suggested recognising that article 8 protected a right to privacy and further warned that, to respond to technological developments, current rules were too limited. The ECtHR itself recognised in 1978 that the text is a living instrument that must be interpreted in the light of present-day conditions (§31),[83] a mode of thinking that continues to upset opponents of the Court and the Convention.[84]

Convention 108 attempted to lay out rules on how privacy should be protected, including principles to follow. The ECtHR has never made a direct reference to Convention 108 in its jurisprudence. Nevertheless, its case law has shown a "move towards the incorporation of the substance of Convention 108 into the interpretation of article 8," according to legal scholar Gloria González Fuster.[85]

The Court's 1987 judgement in *Leander v. Sweden*[86] would become known, according to González Fuster, as a cornerstone of Strasbourg case law on the processing of information about individuals. The case concerned a secret file kept by the Swedish state on a person suspected of being a risk to national security. The EctHR recognised that **an interference with someone's privacy happens when a state authority collects data about them**. It ruled that the person should be able to understand how and when their data might be accessed and used.

2.2. Data protection as a fundamental right

It is the EU that formalised a new right to sit alongside that of privacy: the right to data protection. The challenges arising from new technologies led to the creation of a new fundamental right in the Charter of Fundamental Rights of the European Union.[87] However, as with many developments in EU law, the first steps were taken in relation to the internal market.

2.2.1. Harmonising national practices

In 1995, the EU adopted its first law on data protection, known as the Data Protection Directive. This responded to the different approaches to privacy and data protection adopted by EU member states. The European Commission argued at the time that these divergent approaches could endanger European integration.

The Data Protection Directive was adopted as internal market legislation and sought to facilitate the free flow of personal data between member states.[88] Equivalent protection of privacy and personal data throughout the internal market was the means for achieving that flow. As the preamble notes, approximation of national laws "must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the [European] Community."

In its ruling in *Rundfunk*,[89] the Court of Justice of the EU (CJEU) interpreted the Directive's privacy protections in light of article 8 of the ECHR. **Even though the Directive was adopted under internal market provisions, the Court ruled that it could be applied more broadly**.[90]

The Directive sought uniform standards for processing personal data and exchanging it across borders. It followed many of the standards already laid out in Convention 108, but innovated in others.

It introduced the notion of consent as one requirement for the legitimate processing of personal data. To monitor respect for data protection laws, policies and practice, **the Directive obliged member states to set up an independent supervisory body**. These bodies are referred to as data protection authorities (DPAs).

Four years after the Directive was adopted, the Treaty of Amsterdam extended its principles to the EU institutions and bodies.[91] This led to the creation of the European Data Protection Supervisor (EDPS). The EDPS supervises respect for the right to data protection by EU institutions, agencies, offices and bodies, and assesses the impact of new laws on privacy and data protection rights.

2.2.2. Creating a new fundamental right

The Charter of Fundamental Rights of the EU (hereafter the Charter) was proclaimed on 7 December 2000. However, it did not become legally binding until December 2009, with the entry into force of the Lisbon Treaty. The Charter is inspired by member states' constitutions and also draws upon the ECHR. It includes the right to privacy, and establishes the fundamental right to data protection.

Article 7 of the Charter, on the right to privacy, mirrors article 8 of the ECHR.[92] The key difference is that in the ECHR, a second paragraph lays out under what conditions interferences with the right can be lawful. **In the Charter, article 52 defines how interferences with the right to privacy (and other fundamental rights) can be justified.**

The innovative aspect of article 8 of the Charter, on the right to data protection, lies in its creation of a standalone right. It does not rely on or require association with the right to privacy or other fundamental rights, though in practice this often takes place.

> *Article 8*
>
> *Protection of personal data*
>
> *1. Everyone has the right to the protection of personal data concerning him or her.*
>
> *2. Such data must be processed fairly for specified purposes and*

on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

The Charter applies to all people present on the territory of the EU. In certain circumstances it can apply outside of the physical bounds of Europe. This can be the case with regard to the activities of EU institutions, bodies, offices and agencies abroad; member state implementation of EU law in a non-EU state; or the processing of personal data by non-EU legal entities (examined further in section 2.3.4)

The CJEU has taken an active role in interpreting the rights to data protection and privacy. Niovi Vavoula, an academic and expert in EU data protection law, calls the court the "unlikely hero of data privacy in Europe."[93] However, in its rulings on the impact of new technologies on fundamental rights, the court does not only refer to the rights to data protection or to privacy:

> *...articles 7 and 8 of the EU Charter appear as primordial foundational rights around which most digital rights cases are built. However... there are many Charter rights and freedoms which are or can be a solid foundation to build digital rights strategic litigation.*[94]

As explained earlier, the rights to data protection and privacy require contextual interpretation. Other rights may also be relevant, depending on the particular case. In section 3, we will analyse how the right to an effective remedy has been examined by the CJEU in the context of individual redress for data protection.

2.3. Data protection: definitions and key principles

2.3.1. Defining personal data

Article 4 of the EU's General Data Protection Regulation (GDPR) defines "personal data" as "any information relating to an identified or identifiable natural person ('data subject')." An "identifiable natural person" is:

> *...one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person...*

"Indirect" identification of a person refers to situations where non-personal data can be used to identify a natural person. The issue was examined by the CJEU in a 2024 case, *OC v. European Commission*.[95]

The CJEU has also examined what exactly constitutes personal data. One of the first rulings on the issue was handed down in 2014.[96] A rejected asylum-seeker asked the Dutch authorities for the legal analysis that led to the refusal of his asylum claim, arguing that it constituted personal data about him to which he should have access.

The CJEU considered that the file was an "abstract interpretation of the law" that was not covered by the right of access to personal data. This ruling was not well received by most academic commentators. Frederik Zuiderveen Borgesius and Evelien Brouwer denounced the judgment for expressing "an archaic view of the right to data protection."[97]

The Luxembourg judges had a change of heart in 2017, in the case *Peter Nowak v. Data Protection Commissioner*. They decided that the right of access to personal data "is not restricted to information that is sensitive or private, but potentially encompasses all kinds of

information, not only objective, but also subjective, in the form of opinions and assessments."[98] More information on the right of access is set out in section 3.

2.3.2. Special categories of data

Early in the understanding of privacy, the idea emerged that some personal information deserved more protection than others: special or sensitive categories of data. In Convention 108, a list of special categories of data was proposed. The explanatory report to the convention argued that:

> *...data could require further protection in cases where there is a potential risk of discrimination or injury to an individual's dignity or physical integrity, where the data subject's most intimate sphere, such as his or her sex life or sexual orientation, is being affected, or where processing of data could affect the presumption of innocence.*

The notion emerged, according to academics Paul Quinn and Gianclaudio Malgieri, as a means to an end. **Special or sensitive data requires special protection to try to reduce the possibility of harm, such as discrimination.**[99] The innovation of the EU's 1995 Data Protection Directive was requiring member states to adopt a specific list of five categories of data that warranted special protection. The list included data that revealed:

— racial or ethnic origin;

— political opinions;

— religious or philosophical beliefs;

— trade-union membership; and

— the processing of data concerning health or sex life.[100]

This meant that the processing of that data was prohibited unless justified by a specific legal basis, for example: the explicit consent of the data subject, or a threat to an individual's life (see section 2.3.5).

In the GDPR, EU legislators added three more special categories of data:

— genetic data;

— biometric data; and

— data concerning a person's sexual orientation.

New legal grounds were also added for justifying the processing of data:

— substantial public interest;

— preventive or occupational medicine;

— public health; and

— research for archiving purposes.[101]

The GDPR also prohibits automated decision-making using sensitive personal data unless explicit consent has been obtained.[102] For the purpose of clarifying the spirit of the law, sensitive data can be understood as types of data that have been or could be used to discriminate against and harm individuals.

Dictatorships and other authoritarian regimes have used sensitive data *en masse* to categorise, mistreat, exclude and exterminate individuals based on their race, religion, sexual preferences and health status. It is with noting that beyond the EU, some countries have chosen to add an individual's financial status as sensitive data, a step considered as best practice in the humanitarian sector.

In cases where the processing of special categories of data is "on a large scale," the data controller must appoint a data protection officer and perform a data protection impact assessment (DPIA). Such an assessment, once finalised, will have to be periodically reviewed for as long as the data processing activities it describes exist.

The UK's official guidance for data protection practitioners suggests that every DPIA should be reviewed continuously. The body that formerly brought together data protection authorities from EU member states (now replaced by the European Data Protection Board) considered re-assessment every three years as good practice. However, in later versions of the guidelines this was replaced with an emphasis on continuous review and regular re-assessment, without a fixed timeline.[103]

Sensitive data can also be generated from personal data that would not in and of itself be considered sensitive. For example, posts or activity on Facebook might make it possible to conclude one's sexual preferences, or phone usage data could reveal physical or mental health details. In 2022, the CJEU ruled that generating sensitive data out of 'normal' personal data is prohibited.[104]

2.3.3. The act of processing personal data

The notion of data processing appears innocuous but is in reality central to EU law and the defence of human rights.

In the GDPR, article 4(2) defines processing as:

> *...any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*

In short, one processes data not only when they use data, but also when they do not. For instance, data protection practitioners and regulators will scrutinise how (and if) data is deleted. People processing personal data often assume that once they have deleted a data set, it is permanently gone. This is usually incorrect, as information technology departments are required to ensure data can

be retrieved for the purposes of disaster recovery. Data is only deleted when it is irretrievable from any part of the system.

Another important example is the process of anonymising data, which bears considerable legal and human rights liabilities. Research has found numerous times that the most complex data sets cannot be truly anonymised.[105] This finding led the UK's data protection authority to published guidance on anonymisation.[106]

2.3.4. Controllers and processors

Article 4(7) of the GDPR defines a controller as an entity that:

> *...alone or jointly with others, determines the **purposes and means** of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law. [emphasis added]*

Two or more controllers can determine jointly the purpose and means of processing, a situation known as joint processing. It does not require the participation to be equal.[107]

Identifying a controller is of vital importance for the individual. It is towards the controller that they will seek accountability for the processing of their personal data, including possible compensation in case of violation of their rights.

The controller has to make sure that personal data is held securely. In case an individual wants to access their data, or to rectify or delete any incorrect or unlawful data stored, it is the responsibility of the controller to take action. This issue is discussed further in section 3.

The European Data Protection Board (EDPB) brings together the national data protection authorities of all 27 EU member states. Its guidelines on the right of access state: "Controllers are under the obligation to undertake all reasonable efforts, and put in place the appropriate means, to facilitate the exercise of data subject rights."[108]

In practice, however, identifying the controller may be challenging. An empirical study on the use of personal data gathered from air passengers found that seven countries out of the 11 analysed failed to provide clear information on the identity of the data controller.[109]

Article 4(8) of the GDPR defines a processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller." In other words, the processor follows the instructions of the controller. If a processor fails to do so, they might be held liable in case of harm or failures to comply with legal requirements.

When an individual makes a request for access to the data about them stored by the controller, the responsibility of a processor is, at a minimum, to forward the request to the controller.[110]

2.3.5. Legitimate grounds for processing personal data

Article 6 of the GDPR provides six grounds for lawful processing of personal data:

Consent

Consent is a valid basis for processing, as long as the consent of the individual is freely given, specific, informed and unambiguous. Petra Molnar, a lawyer and researcher, has questioned how consent can be freely given in migration contexts, if it is given under "coercion, even if the coercive circumstances masquerade as efficiency and better service delivery."[111] Indeed, in many cases in the context of migration and asylum, consent cannot provide an adequate basis to justify the processing of personal data.

Contractual obligation

Personal data can be processed if it is necessary for the performance of a contract to which the individual, whose personal data is processed, is party to. This last point is critical, as it obviates the processing of personal data on the grounds of a contract between two other parties alone, for example a company and a public authority.

Legal obligation

Personal data can be processed "if necessary for compliance with a legal obligation to which the controller is subject." This might be the case, for example, if a government passed legislation requiring public or private entities to share data on foreign nationals with the police or immigration authorities.

Vital interests

Protecting the "vital interests of the data subject or of another natural person" can provide a ground for processing personal data. The Spanish data protection authority says that the circumstances "must be real and arise as a result of exceptional and specific situations that could not have been foreseen in advance and excludes any data processing that could be carried out for the regular provision of a service."[112]

Data protection practitioners usually treat this legal basis as only met if an individual's life is at risk and they are unconscious. Its use tends to be exceptional.

Public interest

Processing of personal data is legitimate if necessary "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller."

Legitimate interests

A controller (or third party) must demonstrate three things prior to using their "legitimate interests" as a basis for processing personal data. There are three requirements before relying on the "legitimate interests" ground for processing personal data:

> *1. Purpose test – is there a legitimate interest behind the processing?*

2. Necessity test – is the processing necessary for that purpose?

3. Balancing test – is the legitimate interest overridden by the individual's interests, rights or freedoms?[113]

2.4. Data protection principles

Article 5 of the GDPR sets out six data protection principles:

— lawfulness, fairness and transparency;

— purpose limitation;

— data minimisation;

— accuracy;

— storage limitation; and

— integrity and confidentiality.

The following section explains these principles and analyses how they have been interpreted in the context of migration and asylum.

2.4.1. Lawfulness, fairness and transparency

> *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*

In Greece, where many asylum-seekers are housed **in "Closed Controlled Access Centres", the government has experimented with novel surveillance systems for controlling access and security**. Eleftherios Chelioudakis, executive director of the Greek digital rights organisation *Homo Digitalis*, refers to "an EU-funded, AI-led surveillance ecosystem."[114]

One system (IPERION) is used to store biometric and biographic data on camp residents, staff and visitors. The data is used to control access to the camp, for distribution of food and clothing, and for communicating with asylum-seekers about their applications. The other (KENTAUROS) is geared towards camp security. **Algorithms for automated behaviour analysis are supposed to be able to detect, for example, when a person is acting violently**.

In February 2022, *Homo Digitalis* filed a complaint with the Greek

data protection authority about the systems. The group noted that the government did not conduct a data protection impact assessment before deploying the technologies in the camp, possibly violating the right of the individuals concerned. They also noted that the creation of databases for the systems "is not foreseen by any national legal rule providing the necessary safeguards for the rights of data subjects."[115]

In April 2024, the data protection authority condemned the ministry. It had not conducted an impact assessment of the system or explained to the supervisory authority the potential risks and corresponding mitigation measures. This made it "impossible for the Authority to assess compliance with the principle of lawfulness under Article 5 of the GDPR."[116] The ministry faced a record fine of €170,000. At the time of writing, the technology remains in use.[117]

2.4.2. Purpose limitation

> *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*

The Central Register of Foreign Nationals (*Ausländerzentralregister*, AZR) is a database established in West Germany in 1953. The academic Elisabeth Badenhoop has called it "one of the first comprehensive databases on migrants in the western liberal world."[118]

In 2006, an Austrian citizen filed a complaint with the German courts, which referred the case to the CJEU. The CJEU was asked whether the AZR was compatible with the principle of non-discrimination, as the law required the storage of personal data on all foreign nationals residing in the country for more than three months. The case was concerned with the rights of non-German EU citizens.

The Court held that the purpose of the AZR – to ascertain the right to residence of foreign nationals in Germany – makes the storing and the processing of personal data proportional and lawful. But the Court also found that the processing of AZR data for another purpose, the fight against crime, was not justifiable:

> *While it is true that the objective of fighting crime is a legitimate one, it cannot be relied on in order to justify the systematic processing of personal data when that processing is restricted to the data of Union citizens who are not nationals of the Member State concerned.*[119]

The investigation and prosecution of crimes must take place "irrespective of the nationality of their perpetrators," said the court.[120] Therefore, such a difference in treatment was ruled discriminatory.[121]

In line with this view, the European Commission used to argue that separate databases with discrete purposes were vital for upholding data protection rights. However, over the last decade, its stance has shifted, in particular with **the introduction of new laws opening up asylum and immigration databases to law enforcement agencies**,[122] and making those databases "interoperable" (see section 1.2).

Now, all EU justice and home affairs databases have multiple purposes. The academic Evelien Brouwer considers that "the essence and non-discriminatory approach of data protection have been abandoned for third-country nationals."[123] Nevertheless, provided with the right case, the CJEU might clarify how the principle applies to a new technological context.

Campaign organisations and international organisations have long called for the introduction or maintenance of "firewalls" between different information systems and purposes, to protect people with irregular status. The Council of Europe's European Commission against Racism and Intolerance argues that:

> *...the application of immigration rules must not interfere with the correct application of the human rights obligations of states in respect of all persons in their jurisdiction... There must be clear firewalls which separate the activities of state authorities which*

provide social services and, where applicable, the private sector, from immigration control and enforcement obligations.[124]

There are, however, a growing number of state initiatives to require public and private entities to check people's immigration status, or to report undocumented migrants to the authorities. Early in 2025, the European Commission proposed a new deportation law, which says:

> *Member States shall put in place efficient and proportionate measures to detect third-country nationals who are staying illegally on their territory.*[125]

The *Platform for International Cooperation on Undocumented Migration* has warned that this could be used to abolish or bypass existing firewalls.

2.4.3. Data minimisation

> *Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*

In August 2022, the civil society organisation *Privacy International* launched a court case against the UK Home Office's "collection, processing and sharing of location data of migrants released on immigration bail via the imposition of electronic monitoring (EM) through Global Positioning System (GPS) ankle tags."[126] While the UK may no longer be in the EU, successive governments' undermining of the UK legislation implementing the General Data Protection Regulation requires close scrutiny.[127]

Under the electronic tagging scheme, **the British government obliged migrants who arrived in the UK by boats or other irregular routes, including asylum seekers, to wear a GPS tag at all times.** The practice has been condemned as a form of psychological torture.[128] No clear evidence was provided by the Home Office of its necessity or efficiency.

The system stored all GPS data concerning the person. The UK's data protection authority condemned such an overreaching system:

> *Having access to a person's 24/7 movements is highly intrusive, as it is likely to reveal a lot of information about them, including the potential to infer sensitive information such as their religion, sexuality, or health status.*[129]

The High Court also condemned the scheme for violating the right to privacy. A government report assessing the scheme after it was judged unlawful found that the practice was ineffective.[130] The practice could also exposes tagged people to severe harm in case of a data security failure: it provides constant access to their location.

Nevertheless, in March 2025 the Labour government proposed a legal amendment that would let the Home Office impose electronic tagging on people on immigration bail.[131]

2.4.4. Accuracy

> *Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*

The principle of accuracy plays an essential role in data protection by requiring proactive steps to ensure personal data is accurate (including through audits) and requiring a response to individuals seeking to rectify or delete any inaccurate data.[132] In the case of data processing by public authorities, audits can be done by an in-house data protection officer, or by the independent data protection authorities.

In January 2024, the French data protection authority (*Commission Nationale de l'Informatique et des Libertés*, CNIL) condemned two government ministries for failing to guarantee the accuracy of data

stored about Schengen visa applicants.

French consulates had been copying personal data from the EU's Schengen Information System into a separate national database when a person asked for a visa. However, after auditing national data processing systems, the CNIL admonished the ministry for the practice: it violated EU law and resulted in a mismatch between the European and French systems, which had "difficulty synchronising," leading to the storage and use of inaccurate personal data.[133]

2.4.5. Storage limitation

> *Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*

This principle is **closely related to the principle of accuracy and purpose limitation, and is a core safeguard for the enjoyment of human rights**. It means that information cannot be stored for an unlimited amount of time, the purpose that justified the original processing of the data must still be in place, and that personal data are up-to-date and accurate.

Most (but not all) the EU's large-scale information systems have retention periods of five years, though these can be extended for various reasons.

In the Schengen Information System, alerts can be stored for up to five years before being reviewed.[134] In case a person is banned from entering the Schengen area due to being deemed a security threat, the standards for reviewing the need for the alert are that the person constitutes a genuine, present and sufficiently serious threat.[135] Information about how the individual constitutes a risk should be sufficiently documented to allow for the individual to benefit from an effective judicial remedy.[136]

The maximum period for storage in the Visa Information System, Entry/Exit System and European Travel Information and Authorisation System is also five years.[137] After this point, data should be automatically deleted, though it can be stored for longer in ETIAS if the person gives consent.

Data on asylum applicants can be stored in Eurodac for up to ten years.[138] If the person obtains the nationality of a member state, the information should be deleted.

Each record in the European Criminal Records Information System on Third-Country Nationals will be stored for as long as the data related to the conviction of the person concerned is stored in the national criminal register. The data must be automatically erased upon the expiry of the retention period.[139]

2.4.6. Integrity and confidentiality

> *Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures*

Data security is a key part of data protection. This also encompasses cybersecurity. Organisations that process personal data must take appropriate security measures to ensure it is protected.

In 2011, the EU established an agency known by the abbreviation eu-LISA.[140] Its role is to manage and maintain the EU's large-scale justice and home affairs databases, such as the ETIAS, SIS and VIS. The EDPS, which supervises the agency's compliance with privacy and data protection law, has found multiple failings in its cyber and data security practices.

A journalistic investigation pinned the blame for these failings on eu-LISA's reliance on a private consultancy firm.[141] A breach of the systems' integrity and confidentiality could be catastrophic, potentially affecting millions of people.

2.5. Applicable law

Up to this point, this handbook has mostly referred to the **General Data Protection Regulation (GDPR)**. While this is the best-known, and most widely-applied, piece of EU data protection law, there are two other laws that may be relevant to immigration and asylum practitioners:

— **the Law Enforcement Directive or LED** (Directive (EU) 2016/680);[142] and

— **the Regulation on data protection in EU institutions, agencies and bodies** (Regulation (EU) 2018/1725).[143]

The law that applies in a given case depends on the authority responsible for processing the personal data in question. **The default law in the immigration and asylum context is the GDPR**.

2.5.1. Law enforcement and migration

Initially, European data protection law did not apply to police cooperation and judicial cooperation in criminal matters.[144] In 2010, the European Commission announced it would be taking a new, comprehensive approach to data protection.[145] This would include rules aimed at covering "law enforcement and crime prevention, taking into account the specificities of these areas."[146]

The **Law Enforcement Directive (LED)** was adopted on 27 April 2016, the same day as the GDPR.[147] Both laws entered into force two years later. The GDPR replaced the 1995 Data Protection Directive and imposed common general standards of data protection. The LED set out rules for data protection for law enforcement and judicial cooperation.

The LED includes special limitations to certain data protection rights. These are intended to prevent prejudicing the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, to protect public security or national security, or to protect the rights and freedoms of others. The LED does not apply to national security and other contexts not regulated by EU law, but the Charter of Fundamental Rights and its own set of minimal protection still apply in those contexts.[148]

In the context of migration and asylum, the academic Teresa Quintel has warned that the ongoing criminalisation of migration makes it:

> *...challenging for [law enforcement authorities] to draw a clear line between the scope of application of the GDPR and that of the LED, which creates considerable leeway for competent authorities to apply the Directive to their processing activities.*[149]

She has also warned that law enforcement agencies might choose to use the LED by default, when the opposite should be the case. Indeed, authorities need to justify the application of those more restrictive standards, even in cases involving national security.[150]

2.5.2. European agencies

Another lesser-known EU data protection law is **Regulation 2018/1725**, which was adopted in 2018 and **applies to all personal data processed by EU institutions, agencies, bodies and offices.** The standards are very similar to the GDPR, except in cases where data processing concerns law enforcement and judicial matters. In such cases, special rules apply, which are similar to those in the LED.

EU agencies have taken on a growing role in processing personal data in the context of migration and asylum. This has been the case in particular in so-called "hotspots",[151] where EU agencies and national authorities work together and exchange information on people arriving in EU territory.

The academic Sarah Tas has pointed out that there is not comprehensive supervision of the processing of personal data in the hotspots. Tas also describes how Frontex has taken on an increasing role in gathering intelligence at the border. This did not result in a culture of data protection at the agency,[152] as a scandal in July 2022 on its plan for "intrusive surveillance of migrants" illustrates all too well.[153]

2.6. The proportionality principle

The rights to data protection and privacy are not absolute and may be limited. The jurisprudence of the European Court of Human Rights and of the Court of Justice of the European Union differs in interpreting the limits of those rights and the scope of protection they offer individuals.[154]

2.6.1. The European Court of Human Rights

The right to privacy and its limitations are set out in article 8(2) of the European Convention on Human Rights (ECHR). The article outlines the conditions under which interference with this right is permissible. It must be:

— lawful;

— necessary in a democratic society; and

— serve specific, legitimate purposes.

Once judges at the European Court of Human Rights (ECtHR) recognise that article 8 applies, they will assess whether a measure has been adopted in accordance with the law. The criteria have been fine-tuned by the court. For example, the court has ruled that laws must be accessible to the individual concerned. Thus, they must:

— be of sufficient quality;

— be foreseeable; and

— their consequences must be predictable.

In the 2008 case *Liberty and others v. the United Kingdom*,[155] the ECtHR ruled on a law governing the interception of communications by law enforcement agencies. It said there should be "procedures to be followed for examining, using and storing intercepted material," and that these should be "set out in a form which is open to public scrutiny and knowledge."[156] The quality of law is meant to prevent abuse by officials and to enable its effective control and supervision by the judiciary.[157]

The Court's proportionality assessment, according to academic Lee A. Bygrave,[158] varies according to:

— the gravity of the interference;

— the sensitivity of the information;

— the use made of the data; and

— the safeguards implemented.

For example, states are given less discretion over surveillance measures targeting lawyers and their clients.[159] Privacy in this context is the minimum degree of protection required by the rule of law in a democratic society.[160]

Nevertheless, as in the sphere of immigration and asylum,[161] some argue that the ECtHR is too deferential to state authorities with regard to privacy and data protection. Legal scholars Paul De Hert and Serge Gutwirth have said the court gives authorities:

> *...much leeway. Only flagrant abuse or risky use of data that can easily be used in a discriminatory way is very closely scrutinised, whereas other kinds of processing of data are left untouched 'as long that there is no blood'.*[162]

In the context of migration and asylum

In the context of migration, the vulnerability of the applicant and the special nature of the data processed by the authority should reduce the discretion state authorities have to justify interferences with the right to privacy.

This has been noted in the EDPB's guidance on how to assess the gravity of data breaches. The guidance also says that the level of vulnerability of individuals must now be taken into account to assess the level of risk and due diligence required from controllers.[163]

One question that has come up repeatedly before the ECtHR is the proportionality of the measures used to try to assess the age of asylum-seekers. Where a person does not have an identity document and claims to be a minor, the authorities may request or oblige an age assessment. Medical procedures are one of the most common methods in Europe for doing so.[164] All but two EU member states made use of them in 2018.[165]

The use of medical tests for determining a person's age has faced resounding criticism from the medical, scientific, and human rights communities. The methods used are riddled with scientific uncertainty. For example, a 2019 scientific publication revealed that the ethnicity or origin of the child can influence one of the most common medical methods used by the authorities.[166]

The EctHR ruled in *Darboe and Camara v. Italy*[167] that the Italian authorities should not have used a medical test to assess a person's age. Doing so violated their article 8 rights, as well as the protection of the best interests of the child. The applicant was an "unaccompanied minor living in a migration context that makes him particularly vulnerable," said the judgement.[168] The Italian authorities did not apply the principle of presumption of minor age. They should have granted sufficient procedural guarantees for contesting both the medical assessment and the decision to place the person in an adult centre.

Academic commentators Daniel Simon and Mark Klaassen deplored the court's failure to reduce the discretion of states in using medical methods to assess age.[169] A third-party intervention argued that article 8 should lead the Court to recognise that "all x-ray methods are invasive and too inaccurate to determine whether a person is a minor or an adult."[170]

In decisions from 2025 on the topic (*A.C. v. France*[171] and *F.B. v. Belgium*[172]), the EctHR has nevertheless held to the same line. Rather than assessing "the suitability and validity of the tests themselves," the court "mainly criticises the lack of informed consent," argues the academic Sophie Bols.[173]

In *A.C. v. France*, the court noted that the practice in France was to refer a person for a medical assessment only if they had no identity paper indicating their age, and there was a doubt that they are children. Only then can a medical report be carried out with sufficient procedural safeguards, such as medical reports explicitly indicating the margin of error of the tests used. The decisions attesting to the adulthood of the person should be based on clear and individualised reasoning. Lastly, authorities must provide accurate and accessible information on legal remedies and the time limitations for pursuing them.[174]

In *F.B. v. Belgium*, the ECtHR made clear that the invasive nature of medical tests means they can only be considered necessary and proportionate in a democratic society if they are carried out as a last resort. Other, less intrusive methods for inferring the age of the applicant must be used first.[175]

2.6.2. Court of Justice of the European Union

In the Charter of Fundamental Rights, **article 52 sets out limits for "the exercise of the rights and freedoms recognised by this Charter."** Any measure that impinges upon those rights and freedoms must:

— be provided by law;

— respect the essence of the rights;

— genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others; and

— be necessary and proportionate.

Article 52(3) indicates that the standards provided by the Charter should correspond to the rights guaranteed in the ECHR: "the meaning and the scope of those rights shall be the same," but EU law can provide "more extensive protection."[176]

In 2010, the Court of Justice of the EU (CJEU) noted in the case

Scheke and Eifert[177] that article 6(1) of the Treaty on European Union gave the Charter the same values as the EU treaties. It also ruled that the Charter standards were the minimum available for any person present on EU territory.

The judgment recognised **that the fundamental right to the protection of personal data in article 8 of the Charter is closely connected to the right to respect for private life expressed by article 7, and that both correspond to the standards of the ECHR's article 8**. The Luxembourg judges also made clear that insofar as the Charter contains rights corresponding to the ECHR, they must be similarly interpreted.

In the early 2000s, biometric identification techniques first became widely used across Europe. The interrelation between biometric technology and data protection standards became a recurrent question for supervisory authorities. A report of the predecessor to the European Data Protection Board said: "Proportionality has been the main criterion in almost all decisions taken until now by the Data Protection Authorities on the processing of biometric data."[178]

In other words, biometrics could, in some circumstances, be collected, but only if sufficiently justified. Given the need for proportionality, less intrusive options should be given to individuals in parallel.

In 2004, the case *Schwarz v. Germany*[179] saw the CJEU examine a law forcing every EU citizen to have their fingerprints taken in exchange for obtaining a passport. A German citizen, Mr Schwarz, refused to have his fingerprints taken as he considered it an unjustified violation of his right to privacy.

The CJEU recognised that the collection of biometric data constitutes a threat to the rights to privacy and data protection. Nevertheless, the law was deemed justified because it pursues an objective of general interest: preventing "illegal entry into the European Union."[180]

In the context of migration and asylum

The question of what is strictly necessary and how a measure can affect a person should also be read in light of other rights and the context in which a particular technology is deployed.

Member states of the EU have adopted invasive methods for determining the sexuality of asylum-seekers. Similar to age, the sexual orientation of a person can require special measures to be taken during the asylum procedure, including with regard to the housing facilities provided by the state.[181] Sexual orientation may also be a ground for persecution that can be considered in an application for asylum or subsidiary protection.

In 2013, the CJEU received questions from the Dutch Administrative Supreme Court about the limits imposed by the Charter on methods used to verify the sexual orientation of asylum applicants.[182] Asylum seekers were forced to deal with the most intimate and sordid questions about their sexuality during the interview process. This included a claimant bring asked to bring a home-made pornographic video to their asylum hearing as evidence of their claimed sexual orientation.

The CJEU made clear that "questions concerning details of the [applicant's] sexual practices" are a disproportionate violation of the protection of the right to private life.[183] The judges further stated that asking for or accepting as evidence, "films of [an applicant's] intimate acts" violates human dignity, protected by article 1 of the Charter.[184]

Four years later, the CJEU decided on two new questions in a case referred by the Hungarian courts.[185] The questions concerned the appropriateness of the Hungarian authorities' methods for assessing asylum applicants' sexual orientation.

'F' applied for asylum but was refused protection, a decision based on an expert opinion that said his claim to be homosexual lacked credibility. The assessment was based on a psychological report resulting from several personality tests. The Hungarian court asked

the CJEU if the test respected article 7 (privacy) and article 1 (human dignity), if "no questions are asked about the sexual habits of the applicant for asylum and that applicant is not subject to a physical examination."[186] The test was only conducted after informing the person and obtaining their agreement.

The Luxembourg judges did not think that "the seriousness of the interference with private life" that the psychological tests entailed was justified. Rather, they ruled that such expert reports should be used only if they are based on "sufficiently reliable methods and principles in the light of the standards recognised by the international scientific community."[187] As noted by the academic Iris Goldner Lang, such a report should also be used to "inform and not be decisive for the final decision."[188]

The CJEU also further clarified in this ruling that freely given consent cannot be given in a context where the refusal will constitute an important factor in their asylum claim.[189]

2.6.3. Conclusion

The rulings of the ECtHR and of the CJEU concern different types of technologies and data processing. However, they have both limited the invasiveness of states' actions that infringe upon the right to privacy. They have used different tests to assess whether laws, policies or actions were justified. As noted, some academic commentators have argued that the ECtHR, in comparison to the CJEU, gives too much discretion to states.

In the context of migration and asylum, it is noteworthy that the CJEU, contrary to the ECtHR, has considered the suitability of a given technology – that is, whether it is fit for purpose.[190] The court has established a test relying on "standards recognized by the scientific community" to assess if a measure should be used at all.

CASE STUDY: MOBILE PHONE DATA EXTRACTION

As noted in section 1.2.7, mobile phone data extraction and analysis has become a common practice across several EU member states. An asylum seeker interviewed by the academics Francesca Palmiotto and Derya Özkul expressed how he felt when the authorities demanded his phone: "like handing my whole life over." Whether this highly intrusive practice respects the right to data protection and to privacy has been examined by several courts.

In the Netherlands, the Administrative Supreme Court ruled in 2024 that the practice was not based on adequate legislation and therefore unlawful. The Dutch government had relied on a 2012 law that authorised the migration authorities to search an applicant, including through their phone, for proof of their identity.

But "mobile phones today contain much more personal data," said the court, and are thus "a far-reaching insight into someone's private life" that should be protected against abuse. The judges ordered legal amendments to specify the circumstances in which a mobile phone could be examined.[191]

A year earlier, the Berlin Administrative Court in Germany addressed the same question. German law obliged asylum applicants to hand over their phones if they did not have identity documents. A 2017 law limited the ability to directly access information stored in the phone: officers had to analyse the data via software. This would produce a report indicating the likelihood that the person was of a certain nationality.

In a landmark judgement, the court ruled that the practice violated the principle of proportionality – other, less intrusive measures were not considered before resorting to mobile phone data extraction.[192]

In October 2024, the CJEU had the opportunity to offer more clarity on the proportionality of the practice, though in the context of law enforcement rather than migration and asylum.[193]

The Luxembourg judges first recognised that the seizure and access by the authorities constituted a particularly serious

interference with articles 7 and 8 of the Charter.

However, they ruled that the practice did not need to be confined to serious criminal cases. It could be justified as long as the law defined with sufficient precision the nature or categories of offences concerned, and a national court or independent administrative body was required to examine the necessity and proportionality of the measure.[194]

According to the academic Tiago Sérgio Cabral, the CJEU failed to offer guidance to the bodies that will have to conduct proportionality tests: national authorities and courts.[195] The ruling did not lay out further safeguards for protecting sensitive information stored on the phone of the applicant, or in preventing abuse by officers when they accessed the phone.

In sum, **the jurisprudence on mobile phone data extraction does not forbid the practice as long as it respects standards relating to lawfulness and proportionality**. Nevertheless, many questions remain unanswered on the compliance of the practice with several data protection principles, as well as how judicial authorities will carry out the balancing exercise in individual cases. The CJEU missed an opportunity to set a European standard, instead leaving it to member states or EU legislators to establish a common practice that respects the Charter.

3. Opportunities for redress

The right to data protection has always been put forth by EU legislators as a way to justify the processing of huge amounts of often-sensitive personal data.

However, the question remains whether this is merely a statement of intent or a grant of real rights.

The rights to access, rectify and delete personal data offer people important opportunities for redress, but they can be restricted by the authorities.

In the fields of security, migration and asylum, decisions on this question have too often been secretive and arbitrary.

But a decision of the CJEU; gradual increases in transparency over the enforcement of data protection rights in the EU's huge databases; and litigation, campaigning and journalism, may help to change matters.

3.1. The right of redress

"Everyone" has the right to redress for incorrect, unlawful or illegal processing of their personal data. In this context, "everyone" consists of anyone, anywhere in the world, whose personal data is processed by a controller that is a legal entity in an EU member state. Rights can even be enforced against a processor that is a non-EU legal entity, as long as the data controller they are appointed by is a legality entity in an EU member state.[196]

The right of redress is, then, relatively broad – at least in theory. It is built on three other rights: access, rectification and deletion.

CASE STUDY: CONTROLLERS, PROCESSORS AND REDRESS

A Dutch company pays a Kenyan company to collect data on children in Kenya. The aim is to analyse the effects of a medical treatment. The company in Kenya is processing the personal data for the purposes of the Dutch company. The Dutch entity sets the purposes because it decides what personal data the Kenyan entity collects and why.

People whose data is gathered by the Kenyan company (the processor) can therefore exercise their rights against the Dutch company (the controller). This remains the case even if the Kenyan company only sends the Dutch company aggregated data sets and general lessons learnt out of the data analysis, and not the personal data of individual children.

3.1.1. The right of access

The right of access is set out in **article 15 of the GDPR**. It states, firstly, that a person has the:

> *...right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data.*

Requests for access are sometimes known as **data subject access requests (DSARs).** The law refers to the individual who has personal data about them processed as a "data subject". Article 15 of the GDPR specifies that in response to an access request, the following information should be given to the data subject:

a) the purposes of the processing;

b) the categories of personal data concerned;

c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular in other countries or international organisations;

d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to request from the controller rectification or erasure of personal data, restriction of processing of personal data, or to object to such processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the personal data are not collected directly from the data subject, any available information as to their source;

h) the existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The right of access, then, can be summarised as having three components:

— **confirmation** as to whether or not personal data are being processed;

— **access** to the personal data being processed; and

— **information** on the processing, on the rights of the data subject, and how the data subject can exercise those rights[197]

The controller also has an obligation to inform people about the processing, or potential processing, of their data. For the Schengen Information System, a huge immigration and policing database, the EU has produced a guide on how to exercise the rights of access, rectification and erasure, including a list of authorities responsible for receiving data subject access requests.[198]

The data controller must cooperate with the data subject if the controller cannot identify the information requested. This may involve, for example, asking the data subject for additional information with which to conduct searches for their personal data.

The controller should also comply with the requirements of **article 12 of the GDPR: "Transparent information, communication and modalities for the exercise of the rights of the data subject."** The controller is also obliged to communicate data to the applicant in a "concise, transparent, intelligible and easily accessible form, using clear and plain language."

There is **a deadline of one month for answering a data subject access request**, though two more months can be added in complex cases, or those concerning large amounts of data. Given these timelines, if an individual is seeking rapid access to their personal data, **a request for all of the data held by the controller and/or processor may not be a wise strategy.**

The controller must not delete any information about a person while processing their request for access. The EDPB adds that: "Even

data that may be incorrect or unlawfully processed will have to be provided."[199]

Data controllers must use reasonable efforts to ensure the data subject is the person they claim to be. This may be as straightforward as using an email address already known to the controller. However, controllers have to strike a balance: on one side, the need to ensure accessibility to redress procedures; on the other, the need to know the requester is the person they claim to be. In any case, requests for personal data to verify a data subject's identity should be necessary and proportionate.

3.1.2. The right to rectification

Diana Dimitrova, an academic specialising in data protection, describes the right to rectification as the "enforcement of the principle of data accuracy and completeness."[200] Set out in **article 16 of the GDPR, it allows a data subject to contest any personal data they believe to be inaccurate.**

Inaccuracy refers to information which are not technically or factually accurate. This may include, for example, a misspelt name or information that is unlawfully processed. The exercise of this right might seem rather mundane. However, a simple error in the registration of a person's name can have serious consequences,[201] including deportation.[202]

Rectification may include the addition of a supplementary statement to personal data that is held about a person. For example, a person with the same name as someone listed as 'wanted' in a police database may regularly be stopped at border crossings, or elsewhere. Adding supplementary information to a file could help to prevent this.

3.1.3. The right to deletion

The right to deletion, or erasure, is also known as "the right to be forgotten." In EU law, it first appeared in the 1995 Data Protection Directive. The right is not absolute. There are exceptions related to:

— freedom of expression and information;

— compliance with legal obligations;

— the public interest (for example, public health);

— scientific or historical research purposes;

— statistical purposes; and

— the defence of legal claims.

Its interpretation and scope have evolved over time, in particular with the development of the internet.[203] The "right to be forgotten" is associated with a landmark CJEU ruling against Google.

The judgment introduced an obligation for online search engines to ensure access to the right to deletion. However, as *Access Now*, a civil society organisation defending digital rights, has highlighted:

> *...the Court also left it up to search engines — that is to say private companies — to apply this right and to conduct the very delicate exercise of balancing the right to data protection with freedom of expression.*[204]

Article 17 of the GDPR sets out the reasons an individual may invoke the right to be forgotten:

a) the personal data are no longer necessary for the purposes for which they were collected/processed;
b) consent is the only possible legal basis for the processing, and the data subject withdraws their consent;
c) the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
d) the processing is unlawful;
e) personal data should be erased to comply with a legal obligation; and
f) the personal data concerns a child (under the age of 16) and has been unlawfully processed.

It is up to the controller to decide how to implement this right, in light of available technology and the cost of implementation. They are also responsible for deciding how to best inform other relevant controllers that the data subject has requested deletion.

3.2. Restrictions

Restrictions on the right of access are laid out in article 23 of the GDPR. Restrictions may be permitted for reasons of:

a) national security;

b) defence;

c) public security;

d) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;

e) other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation matters, public health and social security;

f) the protection of judicial independence and judicial proceedings;

g) the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;

h) a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g);

i) the protection of the data subject or the rights and freedoms of others;

j) the enforcement of civil law claims.

Any restrictions should respect the principle of proportionality, as explained in chapter 2. The EDPB also states that to justify a restriction: "the controller must be able to demonstrate that the rights or freedoms of others would be adversely affected in the concrete situation."[205]

The CJEU has ruled that **authorities are obliged to document the reason(s) a restriction has been invoked by a controller, even in cases involving national security.** Courts must be able to make an assessment of the reason(s) invoked by the authority for processing data and restricting access to it.[206]

3.3. Automated decision-making

States and corporations increasingly make important decisions about people solely, or largely, by using computers to process personal data. However, computer software reflects the inequalities, biases and prejudices of the individuals, organisations and societies that produce it.

This problem has led to numerous scandals in recent years, in Europe and elsewhere. The use of algorithms to assist decision-making on visa applications and welfare payments has been particularly prominent.[207]

Article 22 of the GDPR only allows automated decision-making in limited situations, and requires human intervention in decisions that produces legal or significant effects for an individual.

Article 15 of the GDPR lays out special conditions for exercising the right of access in the context of automated decision-making. It also requires the provision of meaningful information about the logic of any algorithms involved and the expected consequences. Legal scholars Goodman and Flaxman argue that this confers a right to explanation to individuals.[208]

The CJEU has issued two rulings on the right of access in the context of automated decision-making: *Schufa Holding*[209] and *Dun & Bradstreet Austria*.[210]

Schufa Holding is a company that processes personal data to assess the likelihood of a person being able to repay a bank loan. It uses that personal data to assign scores to people seeking a loan. A person known as OQ was refused a loan because of the score generated by Schufa. OQ requested access to the data held about them, and the deletion of any incorrect data held by the company.

The company responded by outlining in broad terms the methods for calculating the score. However, they refused to explain the assessment process in detail, citing the need to protect trade secrets contained in copyrighted software. They also argued that they were not responsible for the decision about the loan: they merely provided information to the bank, which made the final decision.

The judges rejected these arguments. They ruled that the score played a determining role in the granting of credit, and that a "decision" could be "a number of acts which may affect the data subject in many ways."

The duty of a controller when responding to a such a request is, according to the CJEU, to:

> *...describe the procedure and principles actually applied in such a way that the data subject can understand which of his or her personal data have been used in what way in the automated decision-making at issue...*

Importantly, the court also ruled that "the complexity of the operations to be carried out in the context of automated decision-making" cannot relieve the controller "of the duty to provide an explanation."

With regard to profiling, the court said that it would be sufficient "to inform the data subject of the extent to which a variation in the personal data taken into account would have led to a different result."

In this decision, the court did not address the argument of Schufa that the applicant's right of access should be disregarded because of their interest in protecting trade secrets. Two years later, the CJEU did examine this argument, in the case *Dun & Bradstreet Austria*.

Like Schufa Holding, Dun & Bradstreet Austria gathers personal data and assigns people scores indicating their financial creditworthiness. CK was refused a contract by a mobile phone operator because, according to a score assigned by Dun & Bradstreet Austria, they were not creditworthy enough.

CK asked for further information about the reasons for the refusal and the logic behind it, but were denied an explanation. The company

argued that this would endanger the copyright on their software.

The court explained that **the right to access underpins other rights granted by the GDPR**,[211] including the right to explanation and the prohibition on automated profiling. The controller had to strike a balance between the interests of the individual and the company by finding "means of communicating personal data that do not infringe the rights or freedoms of others." At a bare minimum, they cannot refuse to provide all information to the data subject.[212]

Lastly, the court ruled that the national judicial authority should analyse the allegedly protected information on behalf of the applicant.[213] This is intended to strike a balance between the individual's interest in an explanation and the company's interest in secrecy. A booklet by the organisation *Privacy Forum* provides further details on how courts have interpreted the GDPR's rules on automated decision-making.[214]

3.4. From access to redress

> *The right of access is one of the core elements of data protection, it is a vehicle for transparency and accountability on how individuals' personal data is processed.*
>
> -Wojciech Wiewiórowski, European Data Protection Supervisor, January 2025[215]

The right of access, like any transparency measure, does not in and of itself create any radical change. But it can play an important role in upholding rights, protecting individuals and enabling scrutiny of powerful institutions. It can be summarised as a right that underpins and amplifies all other data protection rights. With this in mind, it is important to understand its limits and some potential drawbacks.

3.4.1. Filing a data subject access request

This section outlines **essential information to know before filing a data subject access request.** It is based on a handbook published by *European Digital Rights*.[216]

The first thing to consider is the aim of an access request. For example, requests can help to:

— find out what personal data is being processed, and by whom;

— understand the extent of a problem (for example, how many other agencies or institutions an individual's data has been shared with);

— increase scrutiny (by facilitating further requests, advocacy, campaigning or journalism);

— contest unlawful practice (by establishing facts or serving as the basis for redress against the controller and/or processor); and

— grant agency and understanding to affected individuals (by obtaining disclosure on data collected and how it was used).

The access request process may be lengthy. It is also worth noting that

filing a data subject access request may increase scrutiny or 'interest' of the authorities in a particular case or individual. Nevertheless, despite these limits and potential risks, the right of access can play a significant role in seeking redress.

SEEKING REDRESS: A POTENTIALLY LENGTHY PROCESS

Lengthy procedures can be a significant barrier to obtaining access and any subsequent redress. This is particularly the case when several authorities are involved. Frank van der Linde, a Dutch political activist, has extensive experience of this problem.

In 2018, van der Linde requested his file from the police in the Netherlands. The information released showed his information had been shared with Europol and thus, potentially, with multiple other police forces. Seven years later, he has still not had full access to his file, and is now seeking compensation from Europol.[217]

It is also important to note that van der Linde is in a position of relative security compared to others who might seek access to data about them, in particular those in the immigration and asylum systems. Applicants must present a copy of an identity document to file a request with the police.[218] The data protection principle of purpose limitation should prevent the sharing of the access request with other officials or authorities, but the mere risk should be taken into account by people in a vulnerable situation.[219]

3.4.2. Seeking redress

Redress for violations of data protection law can be sought with the entity processing an individual's personal data, or with the national data protection authority. Individuals can also, in parallel to other forms of redress, bring legal proceedings.

Data protection officer

Article 37 of the GDPR requires that the controller and processor designate a data protection officer (DPO) when the processing of personal data:

- is carried by a public authority or body;
- requires regular and systematic monitoring of data subjects on a large scale; or
- concerns special categories of data or personal data relating to criminal convictions and offences.

The nature of the DPO's role is further explained in article 38 of the GDPR. They should be independent from the controller and the processor and should not be given instructions on how to exercise their work. For the CJEU, this functional independence means that they should be protected from unjustified termination of their employment.[220]

The DPO can be contacted by the data subject with regard to the exercise of their rights. Under the law they are bound by secrecy and confidentiality in the performance of their tasks. **Contact details for the DPO must be included in the legal entity's privacy notice on their website.**

Article 39 of the GDPR lays out the tasks of the DPO. They should inform and advise, monitor compliance (in particular vis-à-vis data protection impact assessments), cooperate with the supervisory authority and act as a contact point for the supervisory authority.

A June 2022 judgment of the CJEU, in the case *Ligue des droits humains*, confirmed the importance of DPOs. The judgment called on member states to make sure that DPOs working for public authorities are provided with the material and human resources necessary to carry out their tasks.[221]

The ruling also affirmed that the lawfulness of automated processing for law enforcement purposes "must be open for review" by the DPO, the national data protection authority, and national courts.[222]

National data protection authorities (DPAs)

To guarantee the enforcement of the right to data protection, **article 51 of the GDPR requires that member states set up independent public authorities in charge of monitoring the application of the law**. These are known as national data protection authorities or DPAs.[223]

The tasks of DPAs are laid out in article 57 of the GDPR. Their role includes:

- providing information on people's rights, including by raising public awareness;
- advising member states on legislative and administrative measures;
- responding to individual requests; and
- investigating alleged violations of the law.

Article 77 of the GDPR gives individuals the right to complain to a supervisory authority. There is no charge for filing a complaint with a DPA. Only where requests are manifestly unfounded or excessive can the DPA charge a reasonable fee or refuse to act.

The question of what precisely constitutes "manifestly unfounded or excessive" was examined by the CJEU in Österreichische Datenschutzbehörde. The court ruled that the terms should be interpreted strictly.[224]

In the same case, the court also reminded member states that they are obliged to ensure their DPA has the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of its powers.[225] A 2022 survey found that over 80% of DPAs in the EU were underfunded and faced difficulties carrying out their work as a result.[226]

When the Law Enforcement Directive came into force in 2018, **DPAs were granted the right to carry out checks on the legality of personal data processing by law enforcement authorities**. However, not all EU member states have implemented this requirement.[227]

Judicial authorities

The **right to judicial remedy is set out in article 78** of the GDPR. **Article 79 of the GDPR states that an individual can file a complaint with a court against a supervisory authority decision, or against a controller or processor.**

Judicial authorities are considered to be the last potential site of redress for data protection violations. Nevertheless, judicial redress is "without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority". A person can file a case against a controller or a processor at the supervisory authority while in parallel filing a case in court.

To bring a case for compensation for the unlawful processing of data, an individual can make a request directly to the controller. In case of refusal, they can complain to a court in the controller's country of establishment. When the controller is an EU agency, the individual should seek compensation at the CJEU.[228]

The right to compensation covers any material and non-material damage, including impact on reputation and mental health. This could also cover, in some cases, the time an individual has spent seeking redress for a violation. Frank van der Linde, for example, is seeking compensation from Europol for the five years he has spent seeking access to his file.

Where there are two or more controllers acting jointly, a case can be brought against one, several or all of them. The burden of proof for determining joint responsibility lies with the controller. In the case *Kočner v. Europol*, the CJEU recognised that the individual only had to establish the existence of "unlawful data processing which caused him or her to suffer damage." Attributing responsibility for unlawful processing is not up to the individual.[229]

CASE STUDY: THE SCHENGEN INFORMATION SYSTEM AND DATA PROTECTION RIGHTS

For over three decades, the effectiveness of the right to data protection in one of the world's largest law enforcement and immigration databases – the EU's Schengen Information System (SIS) – was a secret. It was not until 2023, when a new law entered into force, that record-keeping was made mandatory. Every national data protection authority must now produce annual statistics and forward them to the European Data Protection Board (EDPB).

Statewatch made an access to documents request to the EDPB for the national statistics forwarded by national DPAs. The data on Italy is particularly notable. In 2023, the country denied all requests – more than 4,500 – from people seeking access to data about them stored in the SIS. In most cases, the people filing those requests were seeking information about entry bans or deportation orders. These decisions have a profound impact on people's livelihoods and, in some cases, their survival.

The Italian authorities had been systematically lying to people seeking access to their data. A 2021 report said the Italian authorities' standard response to requests was that "the data subject has no entry bans in the Schengen Territory." The evaluation described this as "misleading" in cases where the information was held, but was denied "for instance due to threats to public or national security."[230]

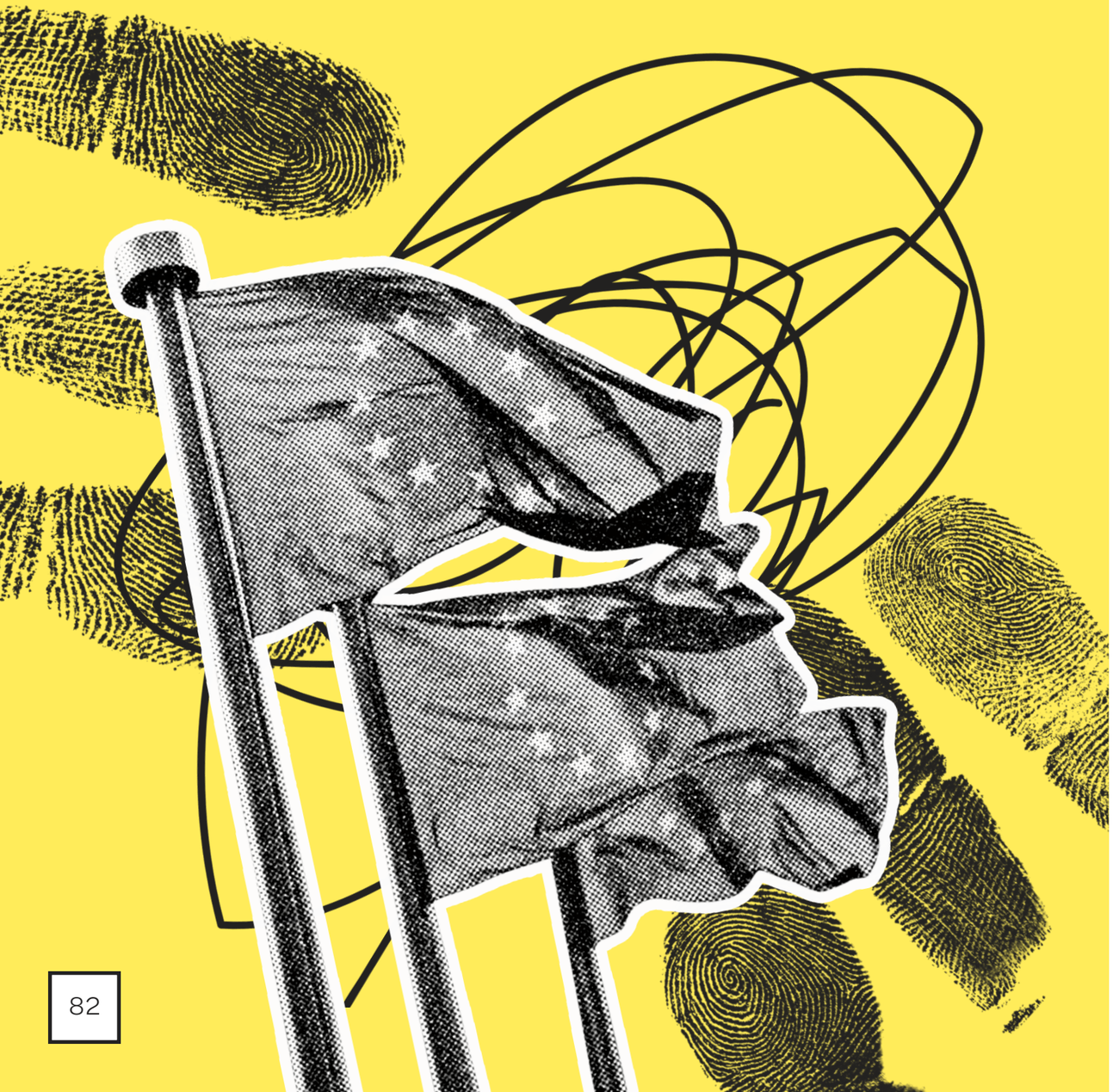
This type of practice recently faced scrutiny in the highest Italian appeal court, in a case that lasted more than 15 years.

Muhamed Dihani was arrested by the Moroccan authorities in 2009 and charged with incitement to terrorism because he campaigned for Western Sahara's independence.[231] He was detained for four years and tortured. After he was released, he tried to reach Italy, to seek treatment and rehabilitation.

He applied for a visa to enter Italy but was refused because of an alert in the SIS: he was deemed a threat to national security because of his

involvement in terrorism. For years, the Italian authorities refused to give access to the file. Judges involved in the case were also denied access to the information.

In January 2025, the Italian Court of Cassation ruled that the entry ban should be discarded due to its basis in the information sent by the Moroccan authorities. This followed a Court of Appeal ruling that said judicial authorities should have the "power to supervise and verify the processing of data, even in contexts related to national security."



Endnotes

1 Petra Molnar, **Technological Testing Grounds: Migration Management Experiments and Reflections from the Ground Up**, EDRi, Refugee Law Lab (November 2020)

2 Anthony Loewenstein, **The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World**, Verso Books (May 2023)

3 Mark Akkerman, **The business of building walls**, Transnational Institute, Stop Wapenhandel, Centre Delàs (November 2019)

4 Angela Giuffrida, Stephanie Kirchgaessner, **Italian government approved use of spyware on members of refugee NGO**, MPs told, The Guardian (March 2025)

5 Christoph Marischka, **European money for the war in Gaza: how EU research funding supports the Israeli arms industry**, Statewatch and Informationsstelle Militarisierung (March 2024)

6 Chloé Berthélémy, Laurence Meyer, **The colonial biometric legacy at heart of new EU asylum system**, EU Observer (April 2024

7 **Council Regulation No 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States**, OJ L 3859.12.2004, pp. 1–6 (December 2004)

8 **EU: MEPs make last-ditch attempt to halt mandatory fingerprinting of all ID holders**, Statewatch (April 2019)

9 Jane Lethbridge, **Privatisation of Migration & Refugee Services & Other Forms of State Disengagement**, Public Services International Research Unit (March 2017)

10 Chris Jones, Romain Lanneau, Yasha Maccanico, **Europe's techno borders**, Statewatch, Euromed Rights (July 2023)

11 **Regulation (EC) No 1049/2001 regarding public access to European Parliament, Council and Commission documents**, OJ L 145, 31.5.2001, p. 43–48 (May 2001)

12 Eleanor Brooks, **What is Freedom of Information: Main Function, Importance, Act Request Guide, Liberties** (July 2022)

13 Border violence monitoring network, **Surveillance technologies at European Borders** (October 2024)

14 Patrick Breyer, **"Video lie detector" for travelers: Patrick Breyer sues EU for keeping the iBorderCtrl project secret** (July 2019)

15 Case C-135/22 P, **Patrick Breyer v. European Research Executive Agency, Appeal Judgement of the Court** (September 2023) paras. 93-94

16 Lilian Tsourdy, **From Tampere 20 to Tampere 2.0: Towards a new European consensus on migration: Chapter 2: EU Agencies**, European Policy Centre (December 2019)

17 Frontex for example, by 2027, will have a standing corps of 10,000 border guards. **European Border and Coast Guard: 10 000-strong standing corps by 2027**, European Parliament (April 2019). An Independent evaluation of EASO noted that the budget of the agency "skyrocketed" since its start of operation: **Independent External Evaluation of EASO's activities covering the period from February 2011 to June 2014**, European Asylum Support Office (December 2015). President Ursula von der Leyen's political guidelines for the next European Commission 2024-2029 set out plans to make Europol a truly operational police agency, and to double its staff: **Europe's choice: political guidelines for the next European Commission 2024-2029, European Commission** (July 2024)

18 Ibid at 16.

19 Ludek Stavinoha, Apostolis Fotiadis, Lola Hierro, **Frontex Unlawfully shared thousands of peoples personal data with Europol**, We are Solomon (July 2025)

20 For example, EU agencies' involvement in research about "security AI". See: Chris Jones, Romain

Lanneau, **Automating authority: Artificial intelligence in European police and border regimes**, Statewatch (April 2025)

21 Lola Hierro, Luděk Stavinoha, Apostolis Fotiadis, **For years, the EU's border agency unlawfully transferred data on migrants and activists to Europol**, El País International (July 2025)

22 Ludek Stavinoha, Giacomo Zandonini, Apostolis Fotiadis, **Europol's deepening aversion to transparency**, EUobserver (May 2025)

23 **Frontex: Billion-euro border agency sues transparency activists**, Statewatch (December 2020)

24 Noah Hatchwell and Pauline F., **Surveillance tech in Serbia**, Border Violence Monitoring Network, Collective aid (November 2024), p.10

25 **Europol, Frontex, EASO, Tackling Migrant Smuggling in the Western Balkans**, Statewatch (February 2020)

26 **Controlled and Confined: Unveiling the Impact of Technology in the Samos Closed Controlled Access Centre**, I have Rights, Border Violence Monitoring Network (January 2025)

27 Elisabeth Badenhoop, **Contextualising Frontex: A Long-Term Perspective on Database Monitoring of Migrants**, Verfassungsblog (February 2020)

28 Romain Lanneau, Chris Jones, **Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe**, Statewatch (April 2025)

29 **Algorithmic video surveillance dangers and counter-**

attacks, La Quadrature du Net

30 Anne Toomey McKenna, **AI mass surveillance at Paris Olympics – a legal scholar on the security boon and privacy nightmare**, The Conversation (July 2024)

31 Philippe Richard, **Après les JO, la vidéosurveillance algorithmique joue les prolongations**, Technique de l'ingenieur (November 2024)

32 **'They never tell us anything' Ongoing data rights violations in the Samos CCAC**, I Have Rights, Homo Digitalis (May 2025)

33 Eleni Stamatoukou, **Greece Expands Non-Transparent Use of Surveillance Tech on Border: NGO**, Balkan Insight (October 2024)

34 See '**Making an application**' in Chris Jones, '**Automated Suspicion: The EU's new travel surveillance initiatives**', Statewatch (July 2020)

35 **Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime**. All UN member states are obliged to set up PNR systems, in accordance with **a 2017 Security Council resolution**

36 Grand Chamber of the CJEU, **Ligue des droits humains**, C-817/19 (June 2022) paras. 194-195

37 Article 4(14) of **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data**, European Parliament and European Council, OJ L 119 (April 2016); article 3(13), **Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detectio**n, the European Parliament and the Council of the European Union OJ L 119, 4.5.2016, pp. 89–131 (April 2016)

38 In the Schengen Convention, this was defined as "Alien for whom an alert has been issued for the purposes of refusing entry." **Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders**, Official Journal L 239 2/09/2000 P. 0019 – 0062 (June 1985)

39 In 2016, the alert on persons concerning article 24 of the SIS II regulation (third country nationals to be refused entry or stay into the Schengen Area) represented 58% of the total alerts on persons: 484,036 alerts. In 2019, the number increased to 527,099, representing 54% of the total alerts on persons. In 2023, there were 600,216 alerts on third country national to be refused entry and stay into the Schengen Area, representing 43% of the total of alerts on persons: eu-Lisa, **Schengen Information System**

40 Council of the European Union, **Commission Working Document: On the return of illegally staying third-country nationals posing a security**, SWD(2024) 287 final (December 2024)

41 Eurodac is short for 'European dactyloscopy'. Dactyloscopy is a term for fingerprinting. Council of the European Union, **Regulation (EC) No 2725/2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention**, OJ L 316 (December 2000)

42 For example, an unaccompanied minor can stay in the member states where he has family members, see: article 8, **Regulation No 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person**, L 180/31 (June 2013)

43 Chris Jones, **11 Years of Eurodac**, Statewatch (January 2014)

44 Civil society organisations as well as the EU's own Fundamental Rights Agency have expressed concern about the reliability of a fingerprint match when a long period of time has passed since a child's fingerprint was first taken. Similar concerns have been raised for facial recognition. See **Fundamental rights implications of storing biometric data in identity documents and residence cards**, European Union Agency for Fundamental Rights (September 2018)

45 Jonathan P. Aus, **Eurodac a solution looking for a problem**, European Integration Online Papers (July 2006)

46 Niovi Vavoula, **Transforming Eurodac from 2016 to the New Pact: From the Dublin System's Sidekick to a Database in Support of EU Policies on Asylum, Resettlement and Irregular Migration**, ECRE (January 2021)

47 European Commission, '**Overview of information management in the area of freedom, security, and justice'**, COM(2010)385 final (July 2010)

48 Sociologist David Lyon theorized in 2009 the notion of the surveillance society by describing surveillance in everyday life. David Lyon, **Surveillance, Power and Everyday Life**. In: Kalantzis-Cope, P., Gherab-Martín, K. (eds) Emerging Digital Spaces in Contemporary Society, Palgrave Macmillan, London (2010)

49 The regulation was adopted in 2013 and came into use in 2015. **Regulation (EU) No 603/2013, Eurodac**, European Parliament and Council of the European Union, OJ L 180 (June 2013)

50 Chapter IV Third-country nationals or stateless persons found illegally staying in an EU Member State, **Regulation (EU) No 603/2013**, Eurodac, European Parliament and Council of the European Union, OJ L 180 (June 2013)

51 Niovi Vavoula, **The 'Puzzle' of EU Large-Scale Information Systems for Third-Country Nationals: Surveillance of Movement and Its Challenges for Privacy and Personal Data Protection**, European Law Review (October 2019).

52 Regulation (EC) No 1986/2006 **regarding access to the Second Generation Schengen Information System (SIS II) by the services in the Member States responsible for issuing vehicle registration certificates**, European Parliament and Council of the European Union OJ L 381 (December 2006).

Regulation (EC) No 1987/2006 **on the establishment, operation and use of the second generation Schengen Information System** (SIS II), European Parliament and Council of the European Union, OJ L 205, (December 2006)

53 **New functions for the Schengen Information System in the fight against terrorism**, Publications Office of the European Union (April 2006)

54 **European Commission, Entry/Exit System (EES),** European Commission (October 2025)

55 ETIAS plans to start operation in the last quarter of 2026, **What is ETIAS**, EU

56 **European criminal records information system – conviction information on third-country nationals (ECRIS-TCN)**, EUR-Lex (May 2023)

57 The others are the European Search Portal, the Multiple Identity Detector (MID) and the shared Biometric Matching System (s-BMS).

58 **Immigration and Privacy in the Law of the European Union: The case of information systems**, p.678

59 Julien Jeandesboz, **Smartening border security in the European Union: An associational inquiry**, Sages Journals, Security Dialogue, *47*(4)92-309, (June 2016)

60 **Fundamental rights and the EU's IT systems for migration and policing**, European Agency for Fundamental Rights (December 2024)

61 Derya Özkul notes in her book: **Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe**, that there is a Latvian speech recognition project for citizenship, p.38

62 An inquiry by political representative Clara Bünger found out that the tool was used to detect Farsi, Dari, Pashto, Iraqi Arabic, Maghrebi Arabic, Levantine Arabic, Gulf Arabic and Egyptian Arabic: Josephine Lulamae, **The BAMF's controversial dialect recognition software: new languages and an EU pilot project**, Algorithm Watch (September 2022)

63 **Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe**, p.46

64 Cecilia Manzotti, **A European language detection software to determine asylum seekers' country of origin: Questioning the assumptions and implications of the EUAA's project**, Sussex Centre for Migration Research Blog (January 2025)

65 **Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe**, pp.36-37

66 **Report criticises widespread electronic monitoring of migrants**, American Bar Association (February 2024)

67 Jo Hynes, Mia Leslie, **'Constantly on edge': the expansion of GPS tagging and the rollout of non-fitted devices**, Medical Justice, Bail for immigration detainees, Public law project (September 2023)

68 Holly Bancroft, **GPS tagging of asylum seekers is ineffective, government report finds**, Independent (January 2025)

69 **Proposal for a regulation 2025/0059 establishing a common system for the return of third-country nationals staying illegally in the Union**, European Commission, COM(2025) 101 final (March 2025), article 31(2)(e)

70 Chris Jones, Jane Kilpatrick, Yasha Maccanico, **Building the biometric state: Police powers and discrimination**, Statewatch (February 2022)

71 Chris Jones, **Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status**, *Statewatch/Platform for International Cooperation on Undocumented Migrants* (November 2019)

72 Dunja Mijatović, **Ethnic profiling: a persisting practice in Europe, the commissioner's human rights comments**, Council of Europe (May 2019); **Addressing racism in policing**, European Agency for Fundamental Rights (2024)

73 Griff Ferris, Sofia Lyall, **New Technology, Old Injustice: Data-driven discrimination and profiling in police and prisons in Europe**, Statewatch (June 2025)

74 **Building the biometric state: Police powers and discrimination**.

75 **Building the biometric state: Police powers and discrimination**, p.10

76 **Synthesis Report for the EMN Focussed Study 2017: Challenges and practices for establishing the identity of third-country nationals in migration procedures**, European Migration Network (December 2017), p.32

77 **From Malpensa to Tel Aviv: Italian police use Israeli software to spy on anti-deportation activists**, Statewatch (February 2025)

78 **Automating Immigration and Asylum: The Uses of New Technologies in Migration and Asylum Governance in Europe**, pp.50-57

79 Author's interview with a refugee support worker in Italy (July 2025)

80 The first holder of the mandate of special rapporteur on the right

to privacy at the United Nations, Joseph Cannataci, explained that privacy needs to be understood in its contextualised application that will differ one from sector of operation to another. In other words, the application of privacy will have a different meaning and understanding if it concerns health or if it concerns migration. The Special Rapporteur further deplored in the same statement to the Human Rights Council of the United Nations that: "a number of powerful states appear to be allergic to anything which in any way could constrain their ability to carry out surveillance in cyberspace." See: Joseph Cannataci, **Special Rapporteur on the Right to Privacy, Statement at the United Nations Human Rights Council** (March 2018)

81 Gloria González Fuster, **The Emergence of Personal Data Protection as a Fundamental Right of the EU**; *Springer International Publishing,* Law, Governance and Technology Series (2014)

82 **Digital Borders and Real Rights**, p.179; **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, pp.55-71

83 European Court of Human Rights, Chamber, **Tyrer v. United Kingdom**, Series A No. 26, application no. 5856/72 (April 1978)

84 See: Professor Richard Ekins' comment in: Michael Cross, **ECHR must evolve, Shabana Mahmood tells Council of Europe ministers**, Law Gazette (June 2025)

85 **The Emergence of Personal Data Protection as a Fundamental Right of the EU**, p.100

86 European Court of Human Rights, **Leander v. Sweden**, *Series A*, no.116, application no. 9248/81 (March 1987)

87 Immigration and Privacy in the Law of the European Union: The case of information systems, p.36; the Comite des Sages, established to reflect on the Charter, found that "new technologies are creating many problems in terms of fundamental rights... the information society may threaten individual privacy": Comité des Sages, **'For a Europe of Civic and Social rights'**, Report by the Comité des Sages

chaired by Maria de Lourdes Pintasilgo, European Commission Directorate-General for Employment, Industrial Relations and Social Affairs (1996); **'Affirming Fundamental Rights in the European Union: Time to Act'**, Expert group on Fundamental Rights (1999)

88 **Directive 95/46/EC of the European Parliament and Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data**, European Parliament and Council of the European Union, L 281 (October 1995)

89 Judgement of the CJEU, Grand Chamber, **Österreichischer Rundfunk and Others**, Joined Cases C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2021:63 (May 2003)

90 **Österreichischer Rundfunk and Others**, paras. 41-42

91 Article 286, **Treaty establishing the European Community** (Amsterdam consolidated version), C 340 (November 1997)

92 **Note from the Praesidium: Subject: Draft Charter of Fundamental Rights of the European Union—Text of the explanations relating to the complete text of the Charter as set out in CHARTE 4487/00 CONVENT 50**, CHARTE 4473/00 CONVENT 49 (October 2000)

93 **Immigration and Privacy in the Law of the European Union: The case of information systems**, p.70

94 **Digital Rights are Charter Rights: Essay Series**, Digital Freedom Fund (September 2023)

95 Judgement of the CJEU, Sixth Chamber, **OC v European Commission**, Case C479/22 P, ECLI:EU:C:2024:215 (March 2024)

96 Judgement of the CJEU, Third Chamber, **YS. and M. and S.**, Joined cases C-141/12 and C-372/12, ECLI:EU:C:2014:2081 (July 2014)

97 Evelien Brouwer, Borgesius Zuiderveen, **Access to Personal**

Data and the Right to Good Governance during Asylum Procedures after the CJEU's YS. and M. and S. judgment, European Journal of Migration and Law, 17(2-3)59-272 (July 2016), p.10

98 Judgement of the CJEU Second Chamber, **Peter Nowak v. Data Protection Commissioner,** C-434/16, ECLI:EU:C:2017:994 (December 2017), para. 34

99 Paul Quinn, Gianclaudio Malgieri , **The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework**, German Law Journal, 22(8):1583-1612, (January 2022)

100 Data Protection Directive, Article 8(1)

101 **Peter Nowak v. Data Protection Commissioner**

102 **YS. and M. and S.**

103 **WP29 issues revised guidelines on Data Protection Impact Assessment (DPIA)**, OneTrust (October 2017)

104 Judgement of the CJEU Grand Chamber, **OT v. Chief Official Ethics Commission**, Case C-184/20, ECLI:EU:C:2022:601 (August 2022)

105 Luc Rocher, Julien Hendrickx & Yves-Alexandre de Montjoye, **Estimating the success of re-identifications in incomplete datasets using generative models**. Nature Communications (July 2019). See also: Marie Douriez , Juliana Freire , Cláudio T. Silva, Harish Doraiswamy, **Anonymizing NYC Taxi Data: Does It Matter?**, International Conference on Data Science and Advanced Analytics (December 2016)**.** Similar to the Belgian UCL study in Nature, this research underscores the near-impossibility of anonymising complex datasets without severely reducing their usefulness.

106 Information Commissioner's Office (ICO), **Anonymisation: managing data protection risk code of practice**, First edition (2012)

107 **Data controller or data processor**, European Data Protection Board

108 **Guidelines 01/2022 of March 2023 on data subject rights - Right of access**, EDPB (March 2023)

109 Plixavra Vogiatzoglou, Katherine Quezada Tavárez, Stefano Fantin et al., **From Theory to Practice: Exercising the Right of Access under the Law Enforcement and PNR Directives**, 11 (2020) JIPITEC 274, (February 2021)

110 Ibid 105, para. 131

111 Petra Molnar, **New technologies in migration: human rights impacts**, Forced Migration Review, FMR 61 – the ETHICS issue (June 2019)

112 **Vital interest and data protection,** Agencia Española de Protección de Datos (October 2024)

113 **'What is the 'legitimate interests' basis?'**, Information Commissioner's Office (February 2025)

114 **Legal bases from the GDPR explained,** Autoriteit Persoonsgegevens (April 2025)

115 **The Hellenic DPA is requested to take action again the deployment of ICT systems IPERION & KENTAUROS in facilities hosting asylum seekers in Greece**, Homo Digitalis (February 2022)

116 **Decision 13/2024**, Hellenic Data Protection Authority (April 2024), para. 24

117 **I HAVE RIGHTS and Homo Digitalis Publish Report on the Situation in the Samos Closed Controlled Access Centre (CCAC) One Year After the Fine Issued by the Hellenic Data Protection Authority for KENTAURUS and HYPERION Systems**, Homo Digitalis (May 2025)

118 Elisabeth Badenhoop, **The fallacy of perfect regulatory controls: Lessons from database surveillance of migration in West Germany from the 1950s to the 1970s**, Regulation & Governance, 15: 952-968

(October 2020)

119 Judgement of the CJEU Grand Chamber, **Heinz Huber v Bundesrepublik Deutschland**, Case C-524/06, ECLI:EU:C:2008:724 (December 2008)

120 **The fallacy of perfect regulatory controls: Lessons from database surveillance of migration in West Germany from the 1950s to the 1970s**, para. 78

121 **The fallacy of perfect regulatory controls: Lessons from database surveillance of migration in West Germany from the 1950s to the 1970s**, para. 80

122 Chris Jones, **Eurodac: Member States want wider police access to biometric database despite most having never made use of it**, Statewatch (December 2016); **Smart borders: Member States seek to make law enforcement access compatible with data retention ruling**, Statewatch (August 2014)

123 **Every Move You Make: The Human Cost of GPS Tagging in the Immigration**, Bail for Immigration Detainee, Public Law Project, Medical Justice, (October 2022)

124 **ECRI General Policy Recommendation N°16 on safeguarding irregularly present migrants from discrimination**, European Commission against Racism and Intolerance (March 2016)

125 **Proposal for a Regulation establishing a common system for the return of third-country nationals staying illegally in the Union, and repealing Directive 2008/115/EC of the European Parliament and the Council, Council Directive 2001/40/EC and Council Decis**, European Commission, COM(2025) 101 final (March 2025)

126 **ICO Complaint against the UK's GPS tagging of migrants**, Privacy International (March 2024)

127 Lorna Cropper and Nuria Pastor, **What do you need to know about the Data (Use and Access) Act 2025?**, Fieldfisher (July 2025)

128 **Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status**

129 **ICO finds the Home Office's pilot of GPS electronic monitoring of migrants breached UK data protection law**, ICO (March 2024)

130 Holly Bancroft, **GPS tagging of asylum seekers is ineffective, government report finds**, Independent (January 2025)

131 Migrant groups reject Labour Government's proposed expansion of "unlawful" and dangerous electronic monitoring, Migrants Organise, (March 2025)

132 Dara Hallinan, Frederik Borgesuis, **Opinions can be incorrect (in our opinion)! On data protection law's accuracy principle**, International Data Privacy Law, 10(1) (February 2020)

133 **Gestion des visas dans l'espace Schengen: la CNIL sanctionne deux ministères,** Commission nationale de l'informatique et des libertés (January 2024)

134 For more details, see articles 53–55, **Regulation (EU) 2018/1862 on the establishment, operation and use of the Schengen Information System (SIS) in the field of police cooperation and judicial cooperation in criminal matters**, European Parliament and Council, OJ L 312 (November 2018); articles 39–40, **Regulation (EU) 2018/1861 on the establishment, operation and use of the Schengen Information System (SIS) in the field of border checks**, European Parliament and Council, OJ L 312 (November 2018)

135 The court ruled in this case against the automatic refusal of entry based on a schengen alert for a family member of a eu citizen. Judgement of the CJEU Grand Chamber, **Commission v. Spain**, Case C-503/03, ECLI:EU:C:2006:74 (January 2006). Different standards apply in term of appeals right for entry bans based on security related concerns, see: Pieter Boeles, Evelien Brouwer, Kees Groenendijk, Eva Hilbrink, Willem Hutten, **Public policy restrictions in EU free**

movement and migration law: General principles and guidelines, Meijer Committee (June 2021)

136 Judgement of the CJEU Grand Chamber, **R.N.N.S & K. A. v Minister van Buitenlandse Zaken**, Joined cases C-225/19 and C-226/19, ECLI:EU:C:2020:951 (November 2020)

137 **EU Agencies and interoperable databases**, Statewatch

138 **Regulation (EU) 2024/1358 on the establishment of 'Eurodac' for the comparison of biometric data**, European Parliament and Council of the European Union, OJ L024/1358 (May 2024), recital 55

139 **Regulation (EU) 2019/816 setting up a centralised system for the identification of Member States holding conviction information on non-EU nationals and stateless persons (ECRIS-TCN)**, European Parliament and Council of the European Union, OJ L 135 (April 2019), articles 8-9

140 The European Union Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice.

141 Olivia Solon, Tomas Statius, **Cybersecurity flaws plagued EU border control system, audit shows**, Bloomberg, Lighthouse Reports (July 2025)

142 **Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data**

143 **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**

144 First a Framework Decision was adopted in 2006 with a limited territorial scope and applying solely to cross-border data processing between the member states. A transitional period came to an end on 1 December 2014. See: Juraj Sajfert and Teresa Quintel, **Data Protection Directive (EU) 2016/680 for Police and Criminal Justice Authorities**, SSRN (December 2017); on the shortcomings of Framework Decision 2008/977/JHA: Paul de Hert and Vagelis Papakonstantinou, **'The New Police and Criminal Justice Data Protection Directive: A First Analysis'**, New Journal of European Criminal Law, 7 (2016)

145 Only with the entry into force of Article 10(1) of Protocol 36 to the 2009 Lisbon Treaty did the Charter come into force.

146 Teresa Quintel, **Data Protection, Migration and Border Control The GDPR, the Law Enforcement Directive and Beyond**, Hart Publishing (May 2024)

147 A Regulation is a binding legislative act and must be applied in its entirety. A directive sets out a goal that EU countries must achieve, but gives them leeway to devise their own laws on how to reach these goals.

148 Judgement of the Court of Justice of the European Union, Grand Chamber, **European Commission and Others v Yassin Abdullah Kadi**, Joined Cases C584/10 P, C593/10 P and C595/10, ECLI:EU:C:2013:518 (July 2013)

149 **Data Protection, Migration and Border Control The GDPR, the Law Enforcement Directive and Beyond**, p.22

150 Court of Justice of the European Union, **Ligue des droits humains (Vérification du traitement des données par l'autorité de contrôle)**, Case C333/22, ECLI:EU:C:2023:874 (November 2023)

151 Katrien Luyten and Anita Orav, **Hotspots at EU external borders State of play**, Briefing, European Parliamentary Research Service (September 2020)

152 Sarah Tas, **Frontex and Data Protection Another Rule of Law**

Challenge in Sight?, Verfassungsblog (September 2022)

153 Luděk Stavinoha, Apostolis Fotiadis and Giacomo Zandonini, **EU's frontex tripped in its plan for 'intrusive' surveillance of migrants**, Balkan Insights (July 2022)

154 **Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data**, EDPS (February 2019).

155 European Court of Human Rights, Fourth Section, **Liberty and others v. the United Kingdom**, application no. 58243/00 (July 2008)

156 Ibid at 153, p.67

157 European Court of Human Rights, Grand Chamber, **Rotaru v. Romania**, App. No. 28341/95 (May 2000), paras. 48-54 and 59; European Court of Human Rights, First Section, **Namazli v. Azerbaijan**, application no. 8826/20 (June 2024)

158 Lee Andrew Bygrave, **Data protection law**, Kluwer Law (January 2003)

159 **Key Theme – Articles 8, 10 and 1 of Protocol No. 1 The rights of lawyers in the Court's case-law**, Registry of the European Court of Human Rights (February 2025)

160 European Court of Human Rights, Grand Chamber, **Kopp v. Switzerland**, no. 23224/94 (March 1998)

161 Anna Lübbe, **The Elephant in the Room**, Verfassungsblog (February 2020); Adel-Naim Reyhani, **Expelled from Humanity**, Verfassungsblog (May 2020)

162 Paul De Hert & Serge Gutwirth **Data protection in the case law of Strasbourg and Luxemburg : constitutionalisation in action** in Serge Gutwirth, Yves Poullet, Paul de Hert, J. Nouwt, & Cecile de Terwangne (Eds.), *Reinventing data protection?*, pp. 3-45

163 **Guidelines 9/2022 on personal data breach notification under GDPR**, European Data Protection Board (April 2023)

164 Non-medical methods involve the use of documents, psychological interviews, estimation based on physical appearance, and assessment by social services. Medical methods vary from carpal (hand/wrist) or collar bone X-ray, dental examination and/or dental X-ray, and sexual maturation observation. The majority of EU member states use carpal/hand wrist X-ray (also known as the Greulich-Pyle Atlas method), whether or not together with other methodologies such as dental observation or dental X-ray. Seven member states (Austria, Croatia, Estonia, Germany, Hungary Italy, Romania) use sexual maturation observation to assess age. Six countries (Croatia, Estonia, France, Germany, Greece, Italy) use psychological interviews. Evelien Brouwer, Romain Lanneau, **Age assessment and the protection of minor asylum seekers: time for a harmonised approach in the EU**, RLI Blog on Refugee law and forced migration (August 2010)

165 **Age assessment and fingerprinting of children in asylum procedures – Minimum age requirements concerning children's rights in the EU,** Fundamental Rights Agency (April 2018)

166 Khalaf Alshamrani, Fabrizio Messina, Amaka C Offiah, **Is the Greulich and Pyle atlas applicable to all ethnicities? A systematic review and meta-analysis**, Eur Radiol, PMID: 30617474 (June 2019)

167 European Court of Human Rights, First Section, **Darboe and Camara v. Italy**, application no. 5797/17 (July 2022)

168 **Is the Greulich and Pyle atlas applicable to all ethnicities? A systematic review and meta-analysis**, para. 151

169 Daniel Simon and Mark Klaassen, **Age assessment and the presumption of minority as a prerequisite for effective human rights protection of asylum seekers: a discussion of Darboe and Camara v. Italy**, Strasbourg Observers (October 2022)

170 **Written intervention in Darboe and Camara v. Italy**, Aire Centre, Dutch Council for Refugees, and the European Council for Refugees

and Exiles (July 2017)

171 European Court of Human Rights, **A.C. c. France**, case 15457/20 (January 2025)

172 European Court of Human Rights, **F.B. c. Belgium**, case 47836/21 (March 2025)

173 **Is the Greulich and Pyle atlas applicable to all ethnicities? A systematic review and meta-analysis**.

174 **Written intervention in Darboe and Camara v. Italy**, paras. 178-180

175 **A.C. c. France**, para. 92

176 **Article 52 Charter**, para. 3

177 Judgement of the Court of Justice of the European Union, Grand Chamber, **Volker und Markus Schecke and Hartmut Eifert v Land Hesse**, joined cases C-92/09 and C-93/09, ECLI:EU:C:2010:662 (November 2010)

178 **Working document on Biometrics**, Article 29 Data Protection Working Party, 12168/02/EN WP 80 (August 2003)

179 Judgement of the Court of Justice of the European Union, Fourth Chamber, **Schwarz v. Germany**, Case C291/12, ECLI:EU:C:2013:670 (October 2013)

180 **Working document on Biometrics**, paras. 37-38, para. 45

181 Steven Blaakman, **Key Challenges faced by LBGI asylum applicants in the EU**, European Parliamentary Research Service (April 2025)

182 Judgement of the Court of Justice of the European Union, Grand Chamber, **A and Others v. Staatssecretaris van Veiligheid en Justitie**, Joined Cases C148/13 to C150/13, ECLI:EU:C:2014:2406 (December 2014)

183 **Key Challenges faced by LBGI asylum applicants in the EU**, para. 64

184 **Key Challenges faced by LBGI asylum applicants in the EU**, paras. 65-66

185 Judgement of the Court of Justice of the European Union, F v. Bevándorlási és Állampolgársági Hivatal, C-473/16, ECLI:EU:C:2018:36 (January 2018)

186 **Key Challenges faced by LBGI asylum applicants in the EU**, para. 26

187 **Key Challenges faced by LBGI asylum applicants in the EU,** para. 58

188 Iris Goldner Lang, **Security-Centric Approach in the Use of Digital Technologies at the EU's External Borders**, *Transnational Legal Theory*, *15*(4), 591–599 (August 2024)

189 **Key Challenges faced by LBGTI asylum applicants in the EU**, para. 53

190 Lorenzo Dalla Corte, **On proportionality in the data protection jurisprudence of the CJEU**, International Data Privacy Law, Volume 12, Issue 4, (November 2022), pp. 259–275

191 **Wet biedt onvoldoende grondslag voor doorzoeken van telefoon zonder toestemming**, Raad van State (April024). For further analysis of the topic, see: Koen Leurs, Rianne Dekker, **The screening of asylum seekers' smartphones at the Dutch border**, Utrecht University (June 2024)

192 Francesca Palmiotto, Derya Ozkul, **"Like Handing My Whole Life Over" The German Federal Administrative Court's Landmark Ruling on Mobile Phone Data Extraction in Asylum Procedures**, Verfassungsblog (February 2023)

193 Court of Justice of the European Union, Grand Chamber, **C.G. v. Bezirkshauptmannschaft Landeck**, Case C-548/21,

ECLI:EU:C:2024:830 (October 2024)

194 **C.G. v. Bezirkshauptmannschaft Landeck**, para. 110

195 Tiago Sérgio Cabral, **Commentary to the Bezirkshauptmannschaft Landeck judgment: a failure by the CJEU in appropriately balancing privacy, data protection and the interests of law enforcement**, Unio EU Law Journal (January 2025)

196 Court of Justice of the European Union, Grand Chamber, **Wirtschaftsakademie Schleswig-Holstein GmbH v Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein**, C-210/16, EU:C:2018:388 (June 2018); Court of Justice of the European Union, **Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV**, Case C-40/17, ECLI:EU: C:2019:629 (July 2019)

197 **Guidelines 01/2022 on data subject rights - Right of access**, European Data Protection Board, Version 2.1 (March 2023)

198 **The Schengen Information System - a guide for exercising data subjects' rights: the right of access, rectification and erasure**, European Data Protection Board, (March 2023)

199 EDPB Guidelines 01/2022, p. 5

200 Diana Dimitrova, **The Rise of the Personal Data Quality Principle. Is it Legal and Does it Have an Impact on the Right to Rectification?**, SSRN (February 2021)

201 See complaints about the recurrence of a misspelt name in Italy: **Accurate, timely, interoperable? Data management in the asylum procedure**, European Migration Network (March 2020).

202 Elspeth Guild, **Unreadable Papers? Biometrics in Practice The EU's first experiences with biometrics: Examining EURODAC**, Wolf Legal Publishers (2007)

203 See the discussion in France that preceded the 2010 adoption of a charter for the right to be forgotten: **Charte du droit à l'oubli dans les sites collaboratifs et les moteurs de recherche**, Secrétariat

d'État chargé de la prospective et du développement de l'économie numérique (October 2010)

204 Eliška Pírková, Estelle Massé, **EU Court decides on two major "right to be forgotten" cases: there are no winners here**, Access Now (October 2019)

205 **Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data**, EDPS (February 2019)

206 Court of Justice of the European Union, **Ligue des droits humains ASBL, BA v Organe de contrôle de l'information policière**, C333/22, ECLI:EU:C:2023:874 (November 2023)

207 David Davidson, Gabriel Geiger, Evaline Schot, Marc Hijink, Saskia Adriaens, May Bulman, Judith Konijn, Allart van der Woude, Ludo Hekman, Daniel Howden, **The algorithm addiction**, Lighthouse Reports (December 2022)

208 Bryce Goodman and Flaxman, **European Union Regulations on Algorithmic Decision Making and a "Right to Explanation"** AI Magazine, 38: 50-57 (September 2017)

209 Court of Justice of the European Union, **OQ v Land Hessen**, Case C634/21, ECLI:EU:C:2023:957 (December 2023)

210 Court of Justice of the European Union, **Dun & Bradstreet Austria**, Case C203/22, ECLI:EU:C:2025:117 (February 2025)

211 The advocate general opinion says it clearly: "the general purpose of the right to obtain information under article 15 GDPR is to enable the data subject to effectively exercise his or her other rights enshrined in the GDPR." See: **Opinion of the Advocate General Richard de la Tour in Dun & Bradstreet Austria**, ECLI:EU:C:2024:745 (September 2024)

212 *Dun & Bradstreet Austria*, para. 72

213 *Dun & Bradstreet Austria*, para. 76

Sebastião Barros Vale and Gabriela Zanfir-Fortuna, **Future of Privacy Forum, Automated Decision-Making Under the GDPR: Practical Cases from Courts and Data Protection Authorities**, Future of Privacy Forum (May 2022)

215 **Coordinated Enforcement Action: EDPS findings highlight challenges on right of access to personal data**, European Data Protection Supervisor (January 2025)

214

216 **How to request access to your personal data stored by Europol : a guide**, European Digital Rights (September 2023)

217 **Activist demands compensation from Europol for illegal surveillance**, Statewatch (June 2025)

218 **EDPB Guidelines on data subject rights access**, 3.1.2 – Form of the request. This would for instance not be necessary in a context where the data subject is someone who wishes to access data held on them by a non-profit organisation from which they receive newsletters. Similarly, if the data subject is a contractor or an employee, making a request via the email address already registered with the employer is often considered sufficient. Once again, data protection is about proportionality. If the request is about medical data, the employer may still request proof of identity.

219 **How to request your personal data stored by Europol: a guide**. See the section on why it is important to file access requests, and the question of "increasing scrutiny of the agency".

220 Court of Justice of the European Union, **Leistritz AG v. LH**, Case C-534/20, ECLI:EU:C:2022:495 (June 2022) paras. 27- 28

221 **Ligue des droits humains**, para. 180

222 **Ligue des droits humains**, para. 179

223 '**Our Members'**, European Data Protection Board, accessed 22 September 2025.

224 It is the duty of the DPA to demonstrate the abusive intention

of the person making the complaint. A large number of requests is only an indication and cannot be automatically classified as excessive above a certain number: Court of Justice of the European Union, **Österreichische Datenschutzbehörde,** Case C-487/21, ECLI:EU:C:2023:369 (May 2023), paras. 56-57

225 **Österreichische Datenschutzbehörde**, para. 51

226 **Data protection: 80% of national authorities underfunded, EU bodies "unable to fulfil legal duties"**, Statewatch (September 2022)

227 **EU states failing to uphold immigration data safeguards amidst renewed push for deportations**, Statewatch (June 2025)

228 Article 268, **Treaty on the Functioning of the European Union**, OJ C 202, 7.6.2016 (December007)

229 Court of Justice of the European Union, Grand Chamber, **Kočner v Europol**, Case C-755/21 P, ECLI:EU:C:2024:202 (March 2024), para. 80

230 **Italian police are "misleading" people about Schengen entry bans, says internal EU report**, Statewatch (February 2025)

231 "**Western Sahara | The United Nations and Decolonization.**", United Nations (September 2024)