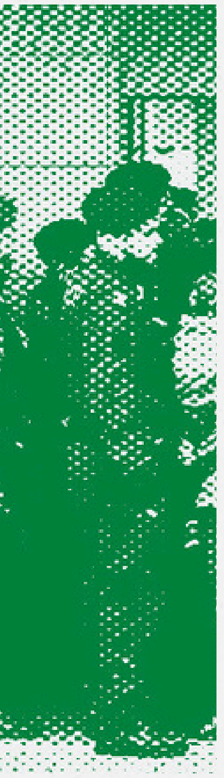


Data protection in immigration & asylum

Rights and opportunities for redress

Romain Lanneau
Statewatch Researcher

May 25

contents

why data protection matters >

data protection: crash course >

opportunities for redress >

discussion >

overview

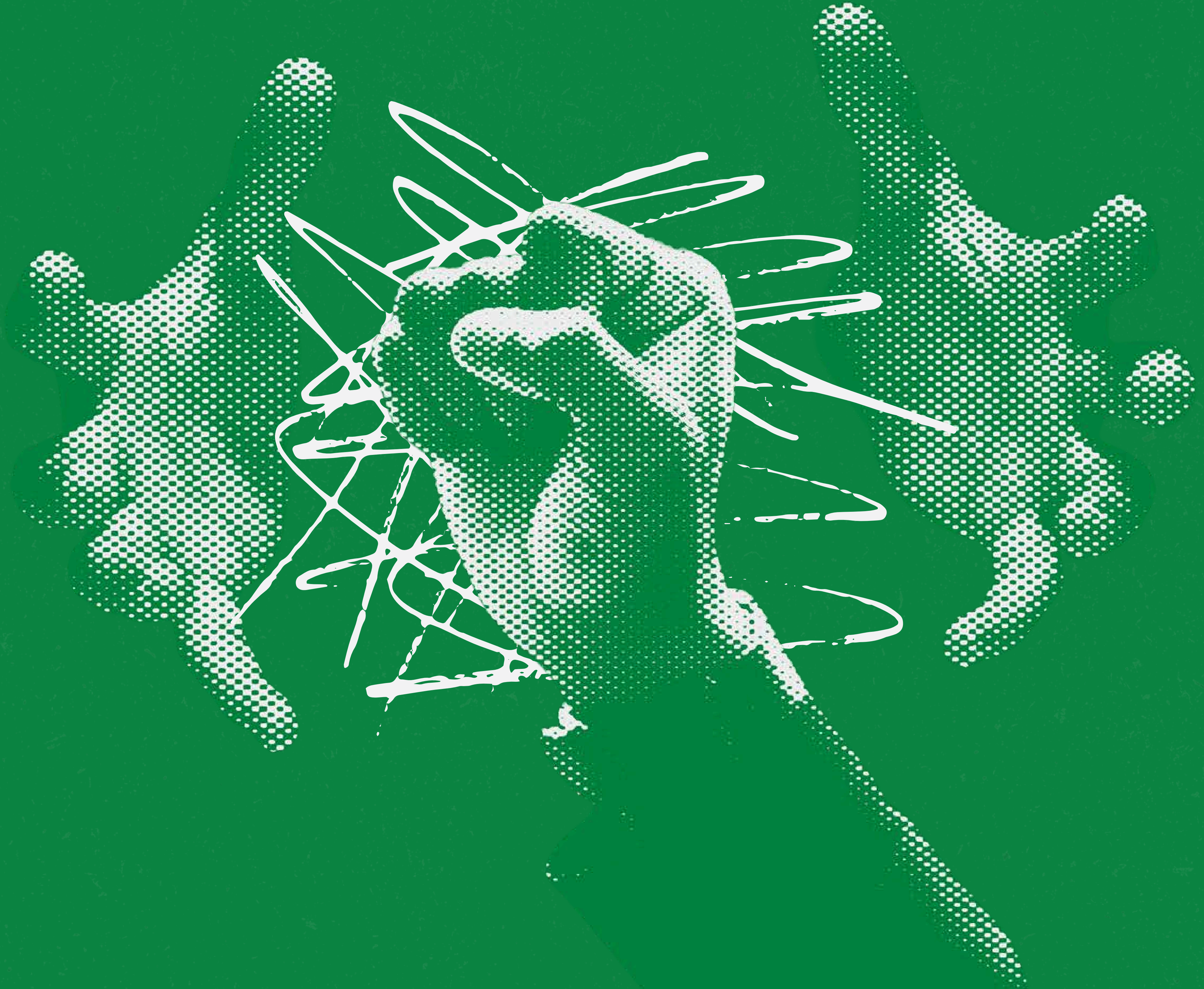
1. the use of digital technologies in migration has expanded enormously

2. data protection offers opportunities for redress and upholding rights

3. individuals should know when authorities are collecting and using their personal data

4. blanket refusals of access to personal data should be challenged

why data protection matters



- migration technologies >
- information systems: a brief history >
- mass data >
- lack of awareness >

question:

when you think about technologies in migration and asylum, what first comes to mind?

Answer in the chat

migration technologies

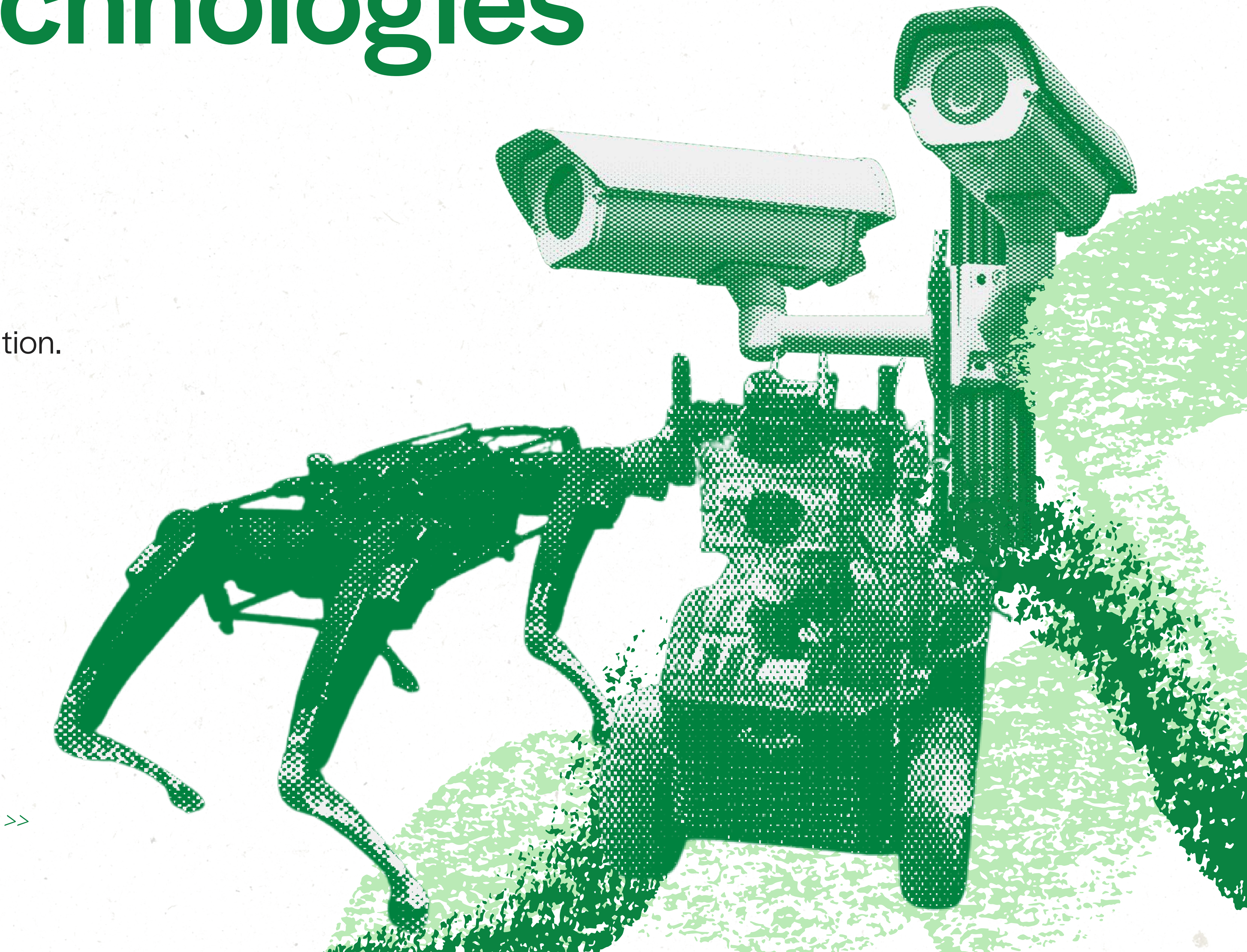
visible technologies

These are what typically come to mind when considering the technologies that control migration.

These include:

- Cameras
- Drones
- E-Gates
- Robots

Automating Immigration and Asylum by Derya Ozkul (2023) >>



invisible migration technologies

before the border

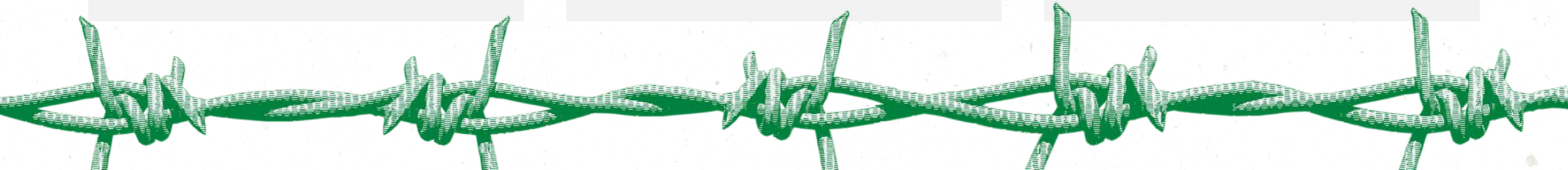
- immigration and displacement forecasting systems
- automated Schengen visa and travel authorisation processing
- employment sponsorship screening

at the border

- risk analysis systems
- document verification technologies
- behaviour and emotion recognition (lie detection) technologies

in the territory

- relocation, settlement or accommodation matching
- appeal case assessments
- electronic monitoring (GPS tagging and facial recognition)
- speech and dialect recognition



information technology systems

three major waves

Niovi Vavoula describes the evolution of information systems in the EU into three phases.

1st wave

1990s to 2001 (Sept. 11)

2nd wave

2000s to early 2010s

3rd wave

2015 to present

IT systems: a brief history

1st wave

1990s to 2001 (Sept. 11)

Infrastructure:

Schengen Information System and Eurodac

Aim:

to prevent unwanted entry into the EU, and to monitor the lawfulness of asylum seekers and irregular migrants within the EU territory

IT systems: a brief history

2nd wave

2000s to early 2010s

Infrastructure:

renewal of existing system and set up of Visa Information System

Aim:

putting large number of individuals under surveillance simply because they pursue everyday activities, such as travel.

IT systems: a brief history

3rd wave

2015 to present

Infrastructure:

EES, ECRIS-TCN, ETIAS, interoperability

Aim:

mobility becomes inherently suspicious

mass data

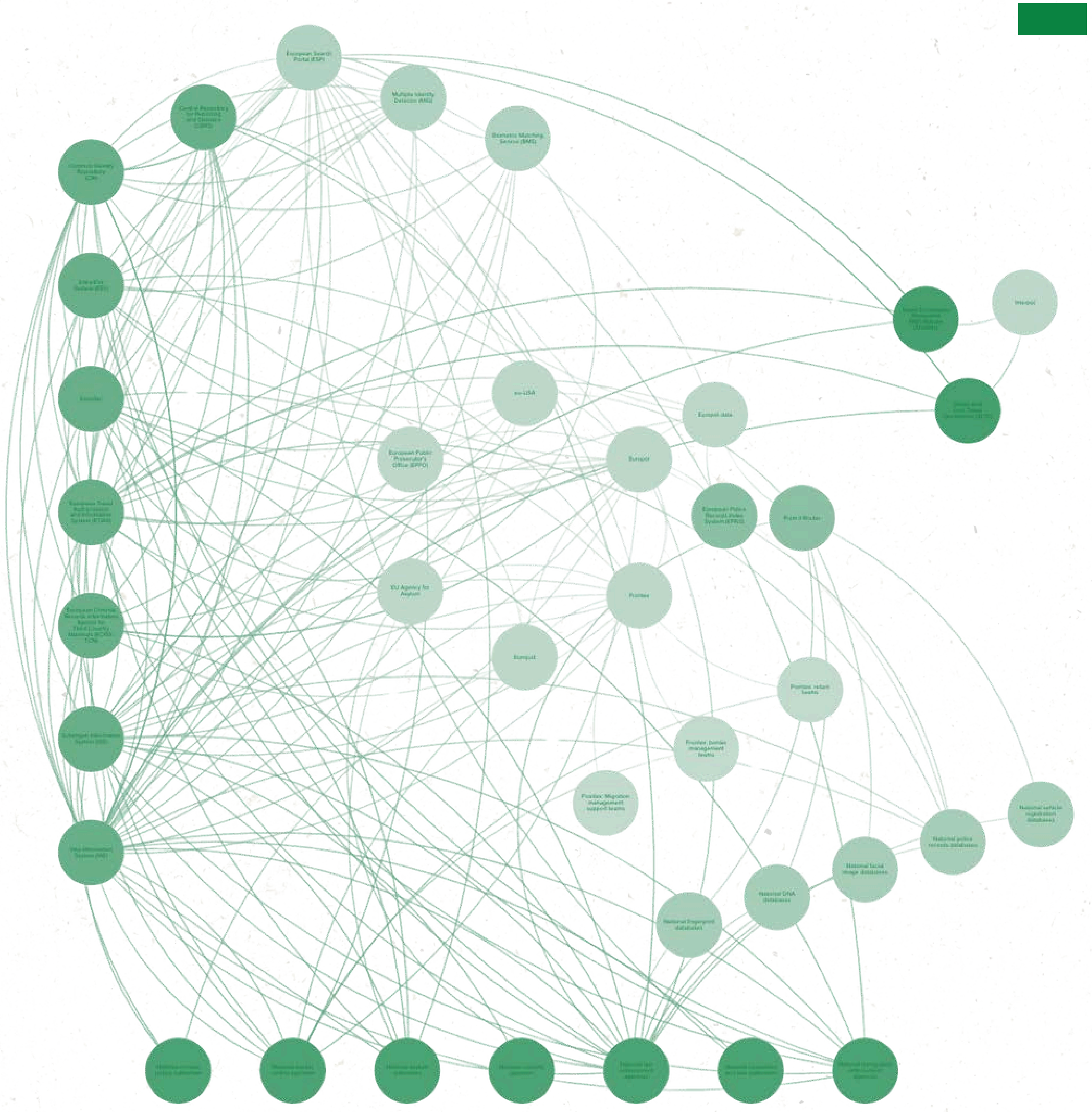
increasing data collection

Data on migrants and asylum seekers has massively expanded with information systems and digital systems used at the border.

use in asylum & migration cases

Data is exchanged between EU agencies, international organisations, third countries and member state law enforcement and migration, asylum authorities.

See our interactive database map >>


European Search Portal (ESP)
Multiple Identity Detector (MID)
Biometric Matching Service (BMS)
Central Repository for Reporting and Statistics (CRRS)
Common Identity Repository (CIR)
Entry/Exit System (EES)
Eurodac
European Travel Authorisation and Information System (ETIAS)
European Criminal Records Information System for Third Country Nationals (ECRIS-TCN)
Schengen Information System (SIS)
Visa Information System (VIS)
eu-LISA
Interpol
Europol data
European Public Prosecutor's Office (EPPO)
Europol
European Police Records Index System (EPRIS)
Prüm II Router
EU Agency for Asylum
Frontex
Eurojust
Frontex return teams
Frontex border management teams
Frontex Migration management support teams
National vehicle registration databases
National police records databases
National facial image databases
National DNA databases
National fingerprint databases

EU AGENCIES AND INTEROPERABLE DATABASES MAP

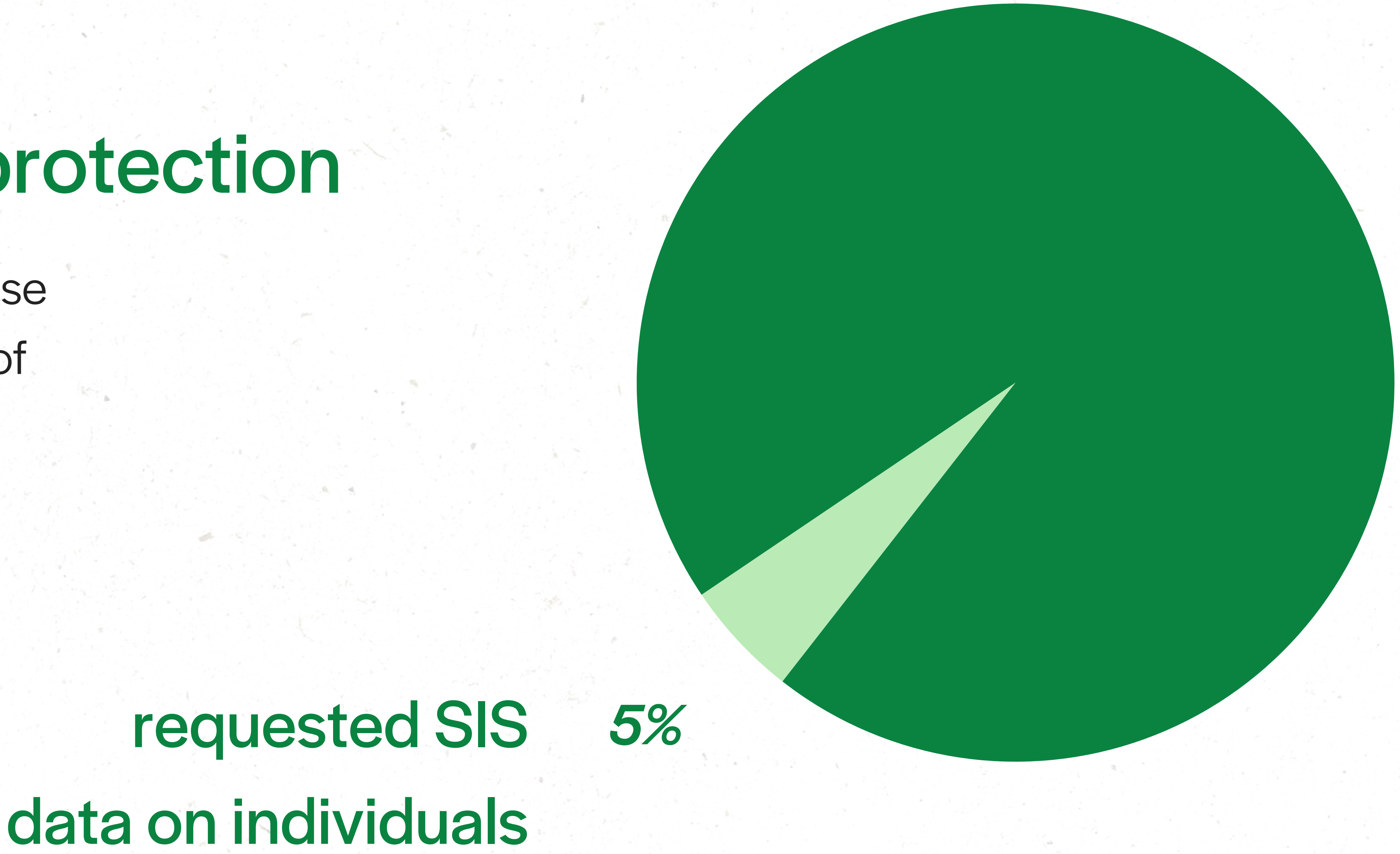
lack of awareness

limited understanding of data protection

Our questionnaire and interviews show that there is no use of data protection and in some cases no understanding of how it can be useful.

little use of current systems

When compared to the amount of data stored, there is a very low number of requests to access that data.



2023 national statistics : access to documents request to the European Data Protection Board (EDPB)

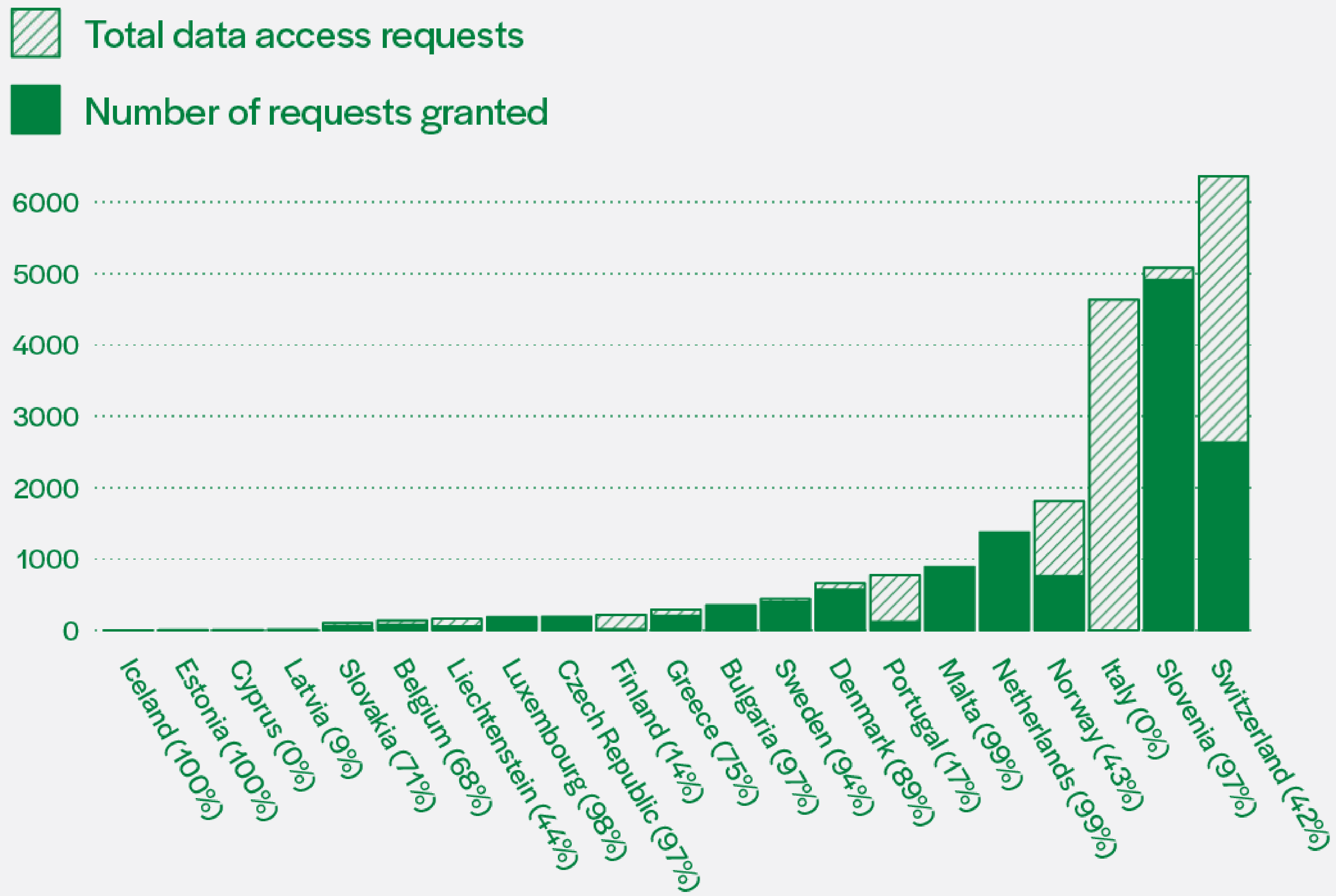
what’s at stake

blatant violations of migrants’ data protection rights

Italy stores most alerts on migrants in the **Schengen Information System (SIS).**

Italian authorities **consistently deny access** on grounds of national security.

They also **lie to applicants** with a response that there are no alerts stored in the system



DATA ACCESS REQUESTS TO SIS DATABASE

questions?

If you have any questions so far or throughout the presentation, please enter them in the chat or raise your hand.

5 minute break

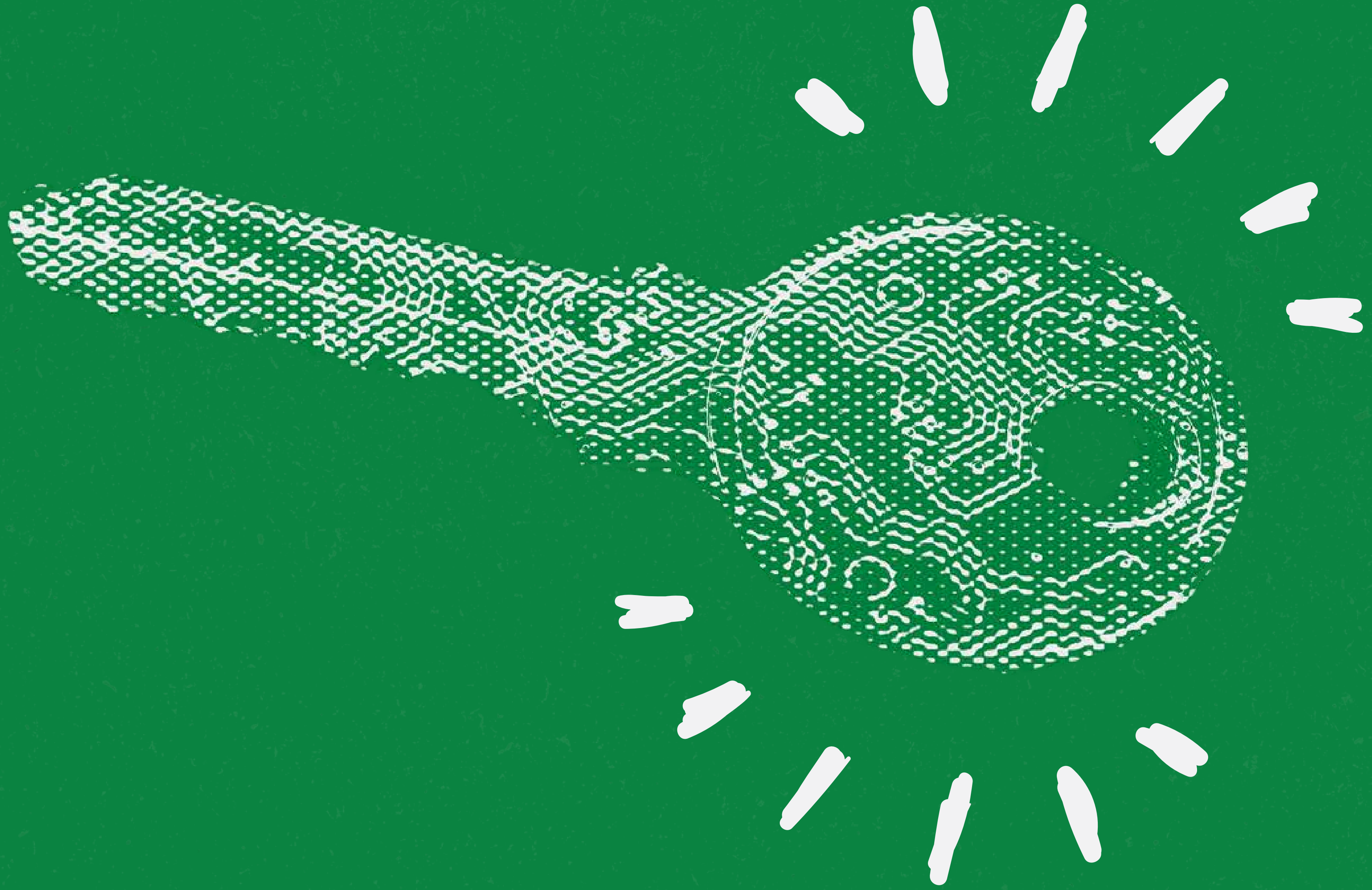
...just enough time to make a donation to Statewatch!

scan to donate

poll:

do you ever use data protection law in immigration or asylum cases?

data protection: crash course



defining data protection >

proportionality principle >

data protection principles >

“

Privacy and data protection are part of the human rights ***too often suspended at the borders*** *of the European Union. As long as we continue treating migration as a ‘problem’, fundamental rights will remain compromised.*

Wojciech Wiewiórowski

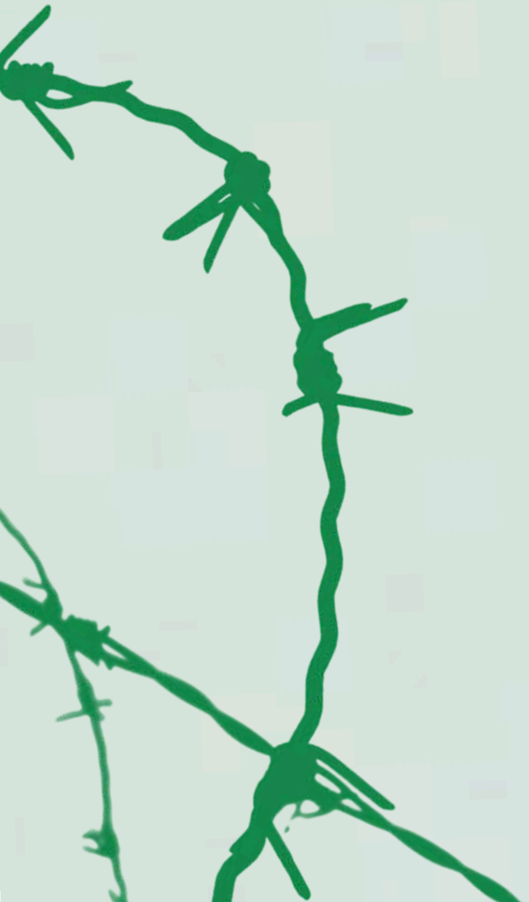
European Data Protection Supervisor
27 January 2023

European Digital Rights
CC BY-SA 2.0

migration & law enforcement

General Data Protection Regulation: standard by default

The default data protection instrument for migration purposes should be the GDPR, according to the EDPB.



criminalisation:

blurring the boundaries

Teresa Quintel argues that migration authorities will apply the most restrictive standards of the Law Enforcement Directive.

Data Protection, Migration and Border Control, Quintel, 2022 >>

Law Enforcement Directive (LED)

This applies when law enforcement authorities process data.

...Except in case of National Security

EU agencies

increasing role in data collection

Agencies such as Frontex, Europol, and EASO are processing more data with limited oversight.

how it is regulated

The regulation is divided into rules similar to GDPR and LED.

Regulation 2018/1725

This EU Regulation protects the processing of personal data by EU institutions, bodies, offices and agencies

Datafication of the hotspots in the blind spot of supervisory authorities by Sarah Tas (2024)
The Origins and Meaning of Data Protection by Douwe and Georges (2020)

defining data protection

“information relating to an identified or identifiable natural person”

Rijkeboer

Case C-553/07 2009

“potentially encompasses all kinds of information, not only objective but also subjective, in the form of opinions and assessments”

Peter Nowak

Case C-434/16 2017

Article 8 of EU Charter of Fundamental Rights >>

proportionality principle

1

lawfulness of invasion

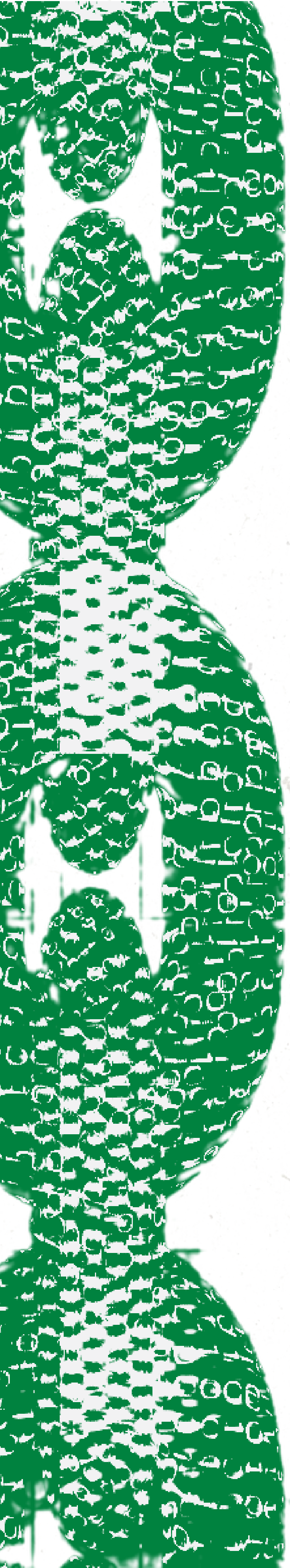
2

balancing of interest

3

documented decision

Article 52 of EU Charter of Fundamental Rights >>



data protection principles

lawfulness

Personal data should be processed lawfully, fairly & in a transparent manner in relation to the data subject.

Case: Smart Camp, Greece 2024 >

data retention

Personal data should be kept for no longer than necessary for processing purposes.

Case: UK v. Marper, ECtHR 2008 >

data minimalisation

Personal data must be adequate, relevant & limited to what is necessary for processing purposes.

UK DPA condems government for GPS tagging of migrants >

accuracy

Personal data must be accurate & up-to-date. Flawed data should be erased or rectified without delay.

French DPA condemns ministry for keeping inaccurate information >

Article 5 paragraph 1 of General Data Protection Regulation (GDPR) >>

data protection principles

purpose limitation

Personal data is only collected for specified, explicit and legitimate purpose and not further processed beyond this

Case: Welfare fraud, the Netherlands 2020 >

- The fraud detection algorithm was banned by the court in 2020 but investigation showed continued use in 2022
- The system relies on many different types of personal data to detect fraud risk
- This resulted in thousands of parents being falsely accused of child subsidy fraud
- Dual nationality was illegally used as a criteria for fraud detection

firewall principle

“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”

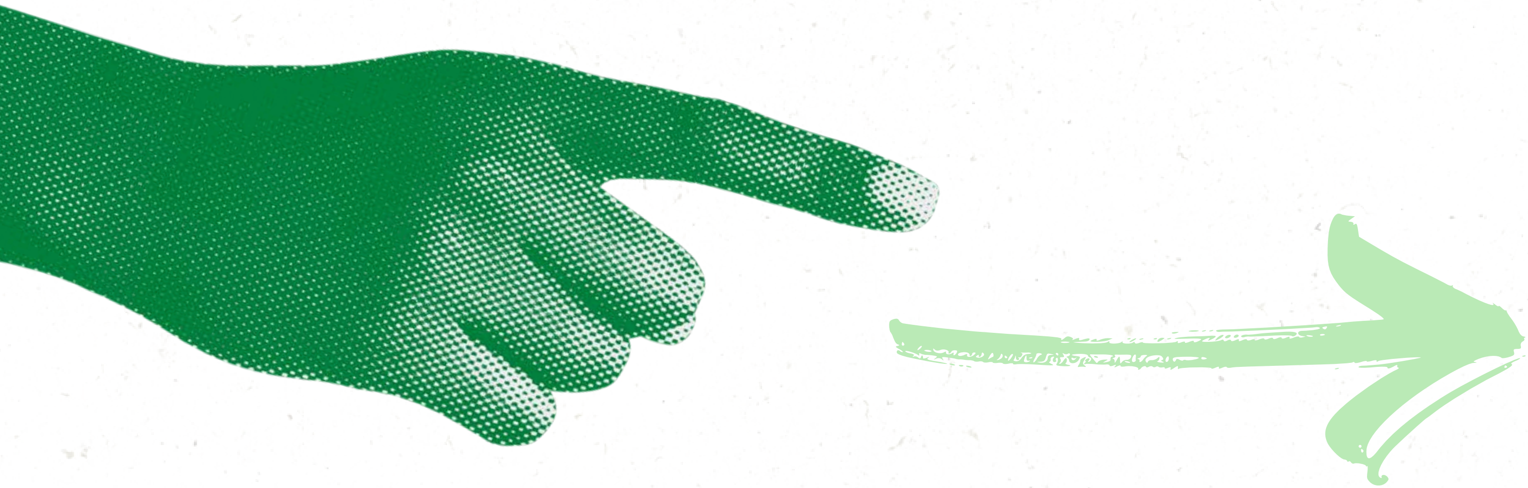
European Commission against Racism and Intolerance (ECRI)

ECRI General Policy Recommendation N°16 >>

third country data

sending data from the EU

- Must respect "essential equivalence of data protection" standards
- Must not violate human rights



receiving data in the EU

- Must come from agreement between law enforcement authorities that assessed fundamental rights
- Must be collected in accordance with human rights laws

interoperable police databases

West African police information system (WAPIS)

- aims to be interoperable with European systems
- threatens the right to leave's one country and to seek asylum

EU Ombudsman decision 2024 >

When spiders share webs 2024 >

case example

mobile phone data extraction

In Country A, all asylum seekers are **required to hand over their mobile phone** for data extraction as part of their application process.

Authorities state that extracting all available data from the phone—including contacts, messages, browsing history, and location data—is **necessary, in all cases, to assess the credibility of asylum claims.**

Asylum seekers are informed that their **consent is required** before the extraction can take place.

questions?

If you have any questions so far or throughout the presentation, please enter them in the chat or raise your hand.

5 minute break

we invite you to use this break to make a donation to Statewatch!

scan to donate

polls:

have you ever filed a data subject access request?

have you sought redress for a data protection violation?

opportunities for redress

data access request >

data controller

restrictions >

accountability in practice >

data subject access request

right of access, rectification, deletion of data

Data subject access requests (DSAR) can be filed with the authority handling the information or directly with the data protection authority

Article 15, 16 and 17 of General Data Protection Regulation (GDPR) >>

access request guides

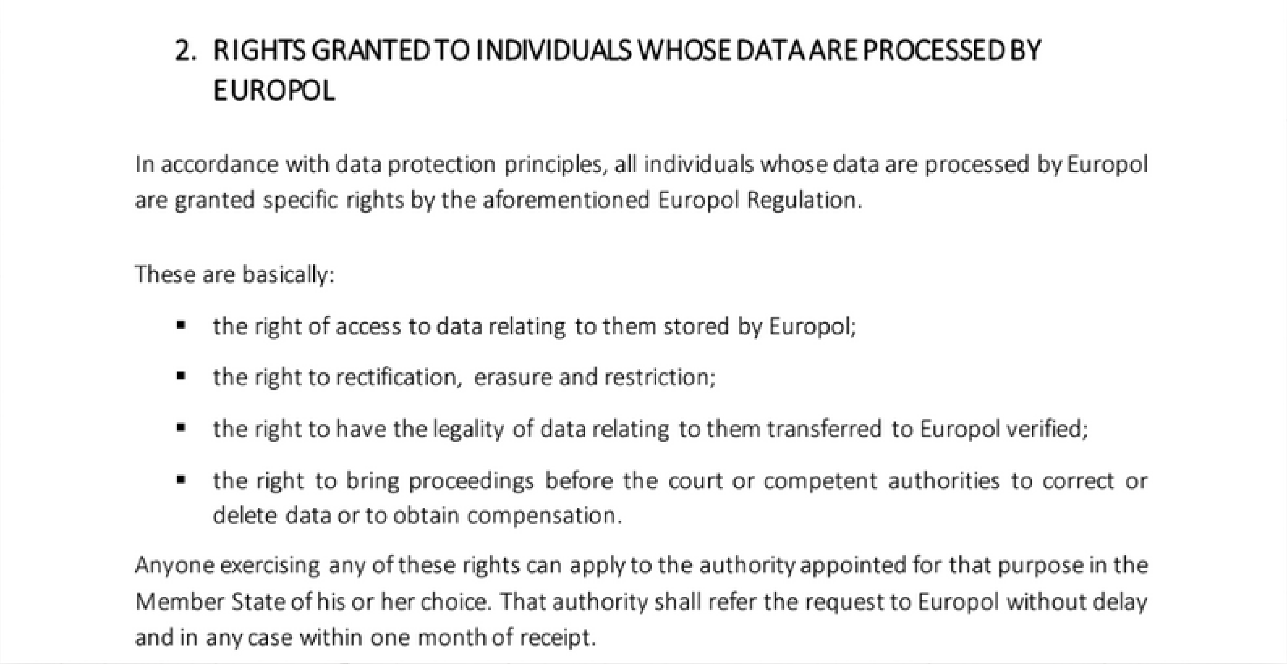
european data protection board

The EDPB has several guides to support the exercise of data protection rights.

Guide for exercising data subjects' rights from Europol >

Guidelines on data subjects' rights >

GUIDE FOR EXERCISING DATA SUBJECT RIGHTS



2. RIGHTS GRANTED TO INDIVIDUALS WHOSE DATA ARE PROCESSED BY EUROPOL

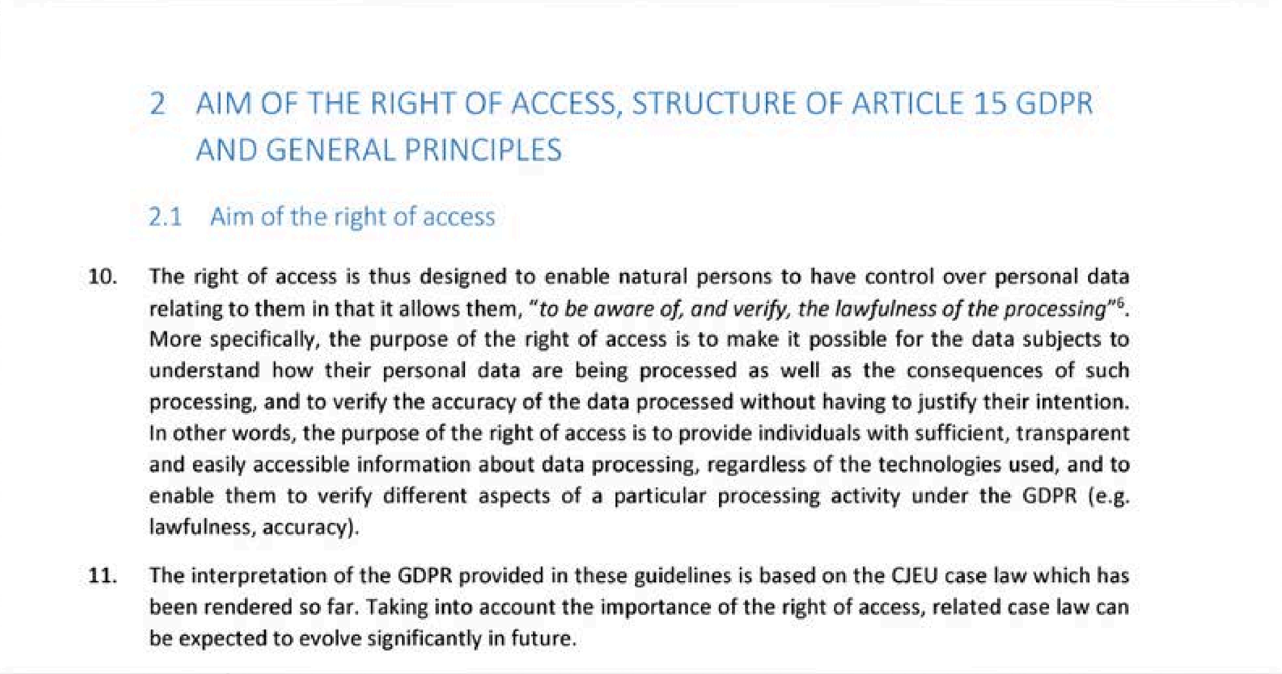
In accordance with data protection principles, all individuals whose data are processed by Europol are granted specific rights by the aforementioned Europol Regulation.

These are basically:

- the right of access to data relating to them stored by Europol;
- the right to rectification, erasure and restriction;
- the right to have the legality of data relating to them transferred to Europol verified;
- the right to bring proceedings before the court or competent authorities to correct or delete data or to obtain compensation.

Anyone exercising any of these rights can apply to the authority appointed for that purpose in the Member State of his or her choice. That authority shall refer the request to Europol without delay and in any case within one month of receipt.

GUIDELINES ON DATA SUBJECTS' RIGHTS



2 AIM OF THE RIGHT OF ACCESS, STRUCTURE OF ARTICLE 15 GDPR AND GENERAL PRINCIPLES

2.1 Aim of the right of access

10. The right of access is thus designed to enable natural persons to have control over personal data relating to them in that it allows them, "*to be aware of, and verify, the lawfulness of the processing*"[6]. More specifically, the purpose of the right of access is to make it possible for the data subjects to understand how their personal data are being processed as well as the consequences of such processing, and to verify the accuracy of the data processed without having to justify their intention. In other words, the purpose of the right of access is to provide individuals with sufficient, transparent and easily accessible information about data processing, regardless of the technologies used, and to enable them to verify different aspects of a particular processing activity under the GDPR (e.g. lawfulness, accuracy).

11. The interpretation of the GDPR provided in these guidelines is based on the CJEU case law which has been rendered so far. Taking into account the importance of the right of access, related case law can be expected to evolve significantly in future.

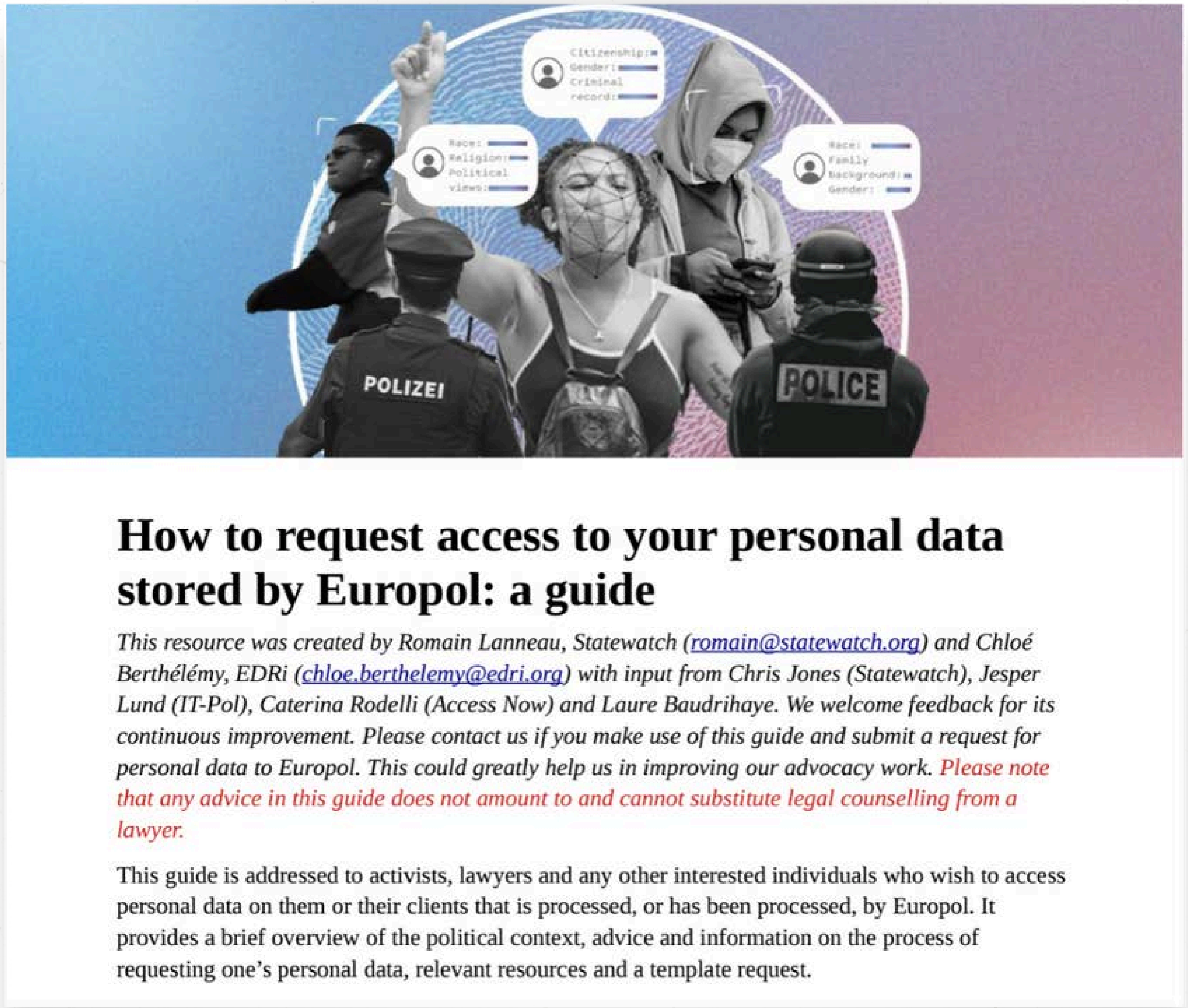
access request guides

European Digital Rights network

EDRi's guide on accessing personal data stored with Europol includes:

- why it is important
- principles and tips
- important information to know
- an email template for sending the request
- how to respond to Europol and remedies

How to request personal data stored by Europol: a guide >



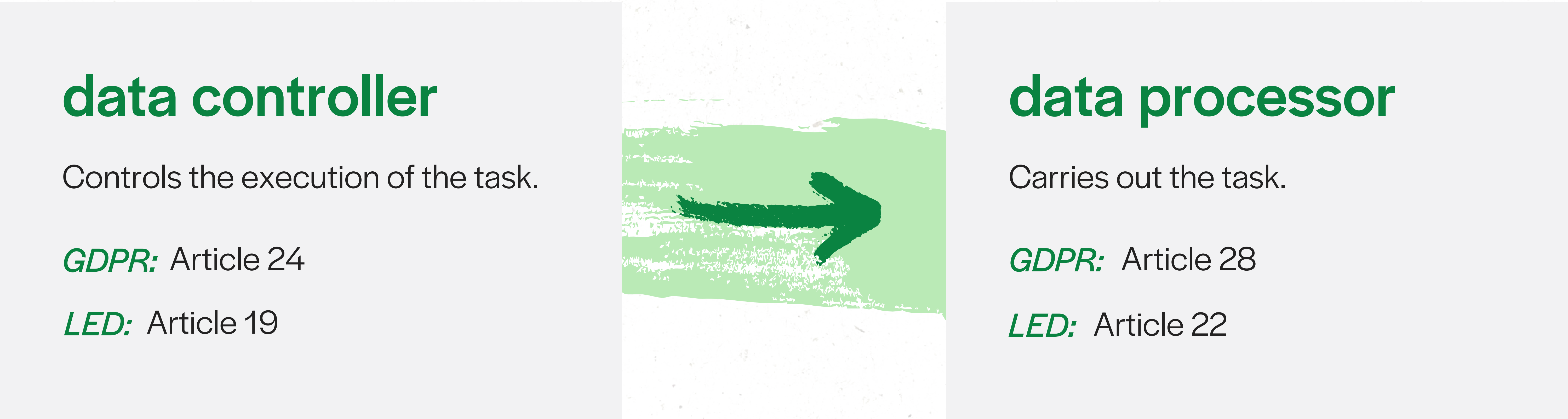
How to request access to your personal data stored by Europol: a guide

This resource was created by Romain Lanneau, Statewatch (romain@statewatch.org) and Chloé Berthélémy, EDRi (chloe.berthelemy@edri.org) with input from Chris Jones (Statewatch), Jesper Lund (IT-Pol), Caterina Rodelli (Access Now) and Laure Baudrihaye. We welcome feedback for its continuous improvement. Please contact us if you make use of this guide and submit a request for personal data to Europol. This could greatly help us in improving our advocacy work. Please note that any advice in this guide does not amount to and cannot substitute legal counselling from a lawyer.

This guide is addressed to activists, lawyers and any other interested individuals who wish to access personal data on them or their clients that is processed, or has been processed, by Europol. It provides a brief overview of the political context, advice and information on the process of requesting one's personal data, relevant resources and a template request.

ensuring compliance

The responsibility for ensuring compliance with data protection principles, including the right of access to data, lies with the data controller.



data controller

Controls the execution of the task.

GDPR: Article 24

LED: Article 19

data processor

Carries out the task.

GDPR: Article 28

LED: Article 22

restrictions

article 23

This covers: national security, public security, prevention, investigations detection or prosecution of criminal offences and more.

article 26

Manifestly unfounded request due to repetitive character. The burden of proof is on the authority.

General Data Protection Regulation (GDPR)

seeking redress

data protection authority

GDPR Article 77

class action

GDPR Article 80

traditional judicial remedy

GDPR Article 79

class action

GDPR Article 80

More information can be found on the collective redress database. >>

accountability in practice

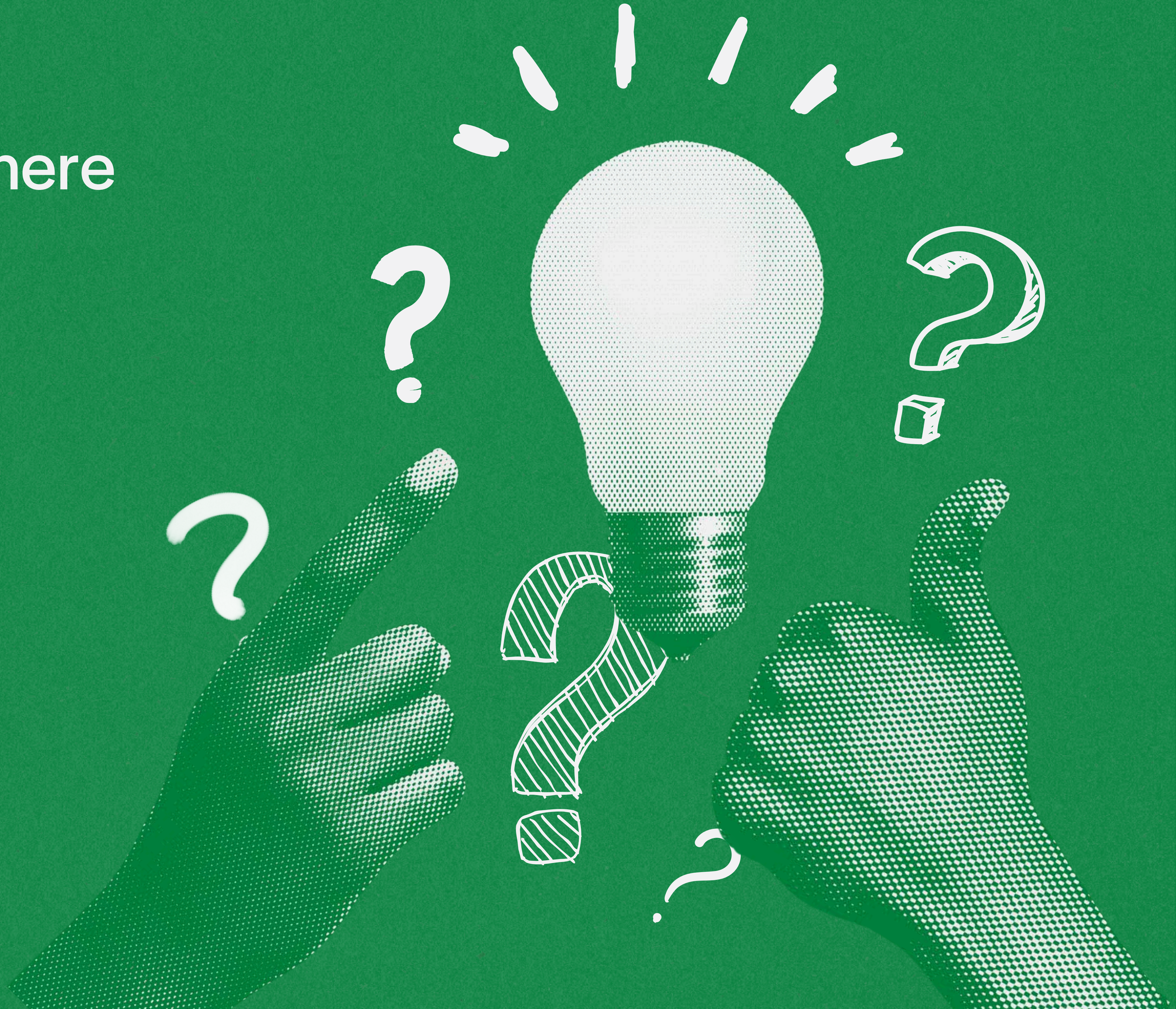
case: Ligue des droits humains (Verification by the supervisory authority of data processing), C-333/22, 2023

Responsibilities of authorities:

- **National authority:** Document reasons to limit right of access.
- **Data protection authority:** Engage in a dialogue with the authority to decide necessary information for data subject to exercise right to effective remedy.
- **Court:** Examine all grounds and evidence for the authority to lawfully process data and restrict access to it.

discussion

do you have examples of cases where you have used or could have used data protection law?



thanks for joining

please take the time to fill out the survey to help us improve future trainings.

For any follow-up questions or to discuss options for private training opportunities, email romain@statewatch.org

become a friend of statewatch

by making a monthly contribution,
you'll join a network of our supporters
who make our work possible.

scan to
donate