Preventing unlawful profiling today and in the future: a guide

FRA
EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

***Europe Direct is a service to help you find answers
to your questions about the European Union***

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels
    may charge you).

Preventing unlawful profiling today and in the future: a guide

Contents

Figures and tables

Abbreviations and acronyms

CCC	Common Core Curriculum
CJEU	Court of Justice of the European Union
DPIA	Data Protection Impact Assessment
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EES	Entry/Exit System
ENISA	European Union Agency for Network and Information Security
ETIAS	European Travel Information and Authorisation System
EU	European Union
EU-MIDIS	European Union Minorities and Discrimination Survey
FRA	European Union Agency for Fundamental Rights
FRONTEX	European Border and Coast Guard (also EBCGA)
GDPR	General Data Protection Regulation
IT	Information Technology
OHCHR	Office of the United Nations High Commissioner for Human Rights
OSCE	Organization for Security and Co-operation in Europe
SIS II	Schengen Information System
TCN	Third Country National
UN	United Nations
UNHRC	United Nations Human Rights Committee
VIS	Visa Information System
WP29	Article 29 Data Protection Working Party

Introduction

Technological developments have triggered an increased use of profiling in a wide range of contexts, including marketing, employment, health, finance, law enforcement, border control and security. The use of profiling tools to support the work of law enforcement and border management officials has received greater attention from EU Member States in recent years. Profiling is commonly, and legitimately, used by law enforcement officers and border guards to prevent, investigate and prosecute criminal offences, as well as to prevent and detect irregular immigration. However, unlawful profiling can undermine trust in the authorities, in particular in the police, and stigmatise certain communities. This in turn can escalate tensions between communities and law enforcement authorities for what is perceived as the discriminatory use of profiling.

This guide explains what profiling is, the legal frameworks that regulate it, and why conducting profiling lawfully is not only necessary to comply with fundamental rights, but also crucial for effective policing and border management. The guide also provides practical guidance on how to avoid unlawful profiling in police and border management operations. The principles and practices in the guide are supported by examples, case studies and case law from across the EU and beyond.

Why do we need this guide?

Profiling raises a number of fundamental rights concerns.[1] Profiling practices risk violating well-established legal principles including equality and non-discrimination, and the rights to respect for private life and data protection. In addition, questions

---

[1]   See FRA (2018e), pp. 85-87; FRA (2017c), pp. 88-89; and FRA (2016), pp. 83-85.

have been raised about its effectiveness in combating illegal activity, as well as possible negative consequences for relations between the authorities (including the police and border management) and the communities they serve.

In response to these concerns, the European Union Agency for Fundamental Rights (FRA) published the guide *Towards more effective policing, Understanding and preventing discriminatory ethnic profiling* in 2010. Focusing on the use of profiling by the police, it concentrated in particular on the exercise of stop and search powers. The guide aimed to give mid-level officers tools for avoiding discriminatory profiling based on ethnicity.

Since then, technological developments have changed the nature of profiling considerably. Much profiling is now based on the results of computer analysis of large data sets. On the legal side, the reformed – stricter – data protection rules applying across the EU from May 2018 set new standards for the collection, analysis and use of personal data.

This updated guide takes account of these significant changes to build on and expand the 2010 guide to reflect the new legal and practical realities. It takes a more comprehensive approach to unlawful profiling by incorporating:

- profiling in the context of border management;
- discriminatory profiling on all grounds, including nationality, age and gender, in addition to ethnic origin; and
- algorithmic, or computer-based, profiling.

This 2018 version also contains new examples and case studies to reflect developments and innovations concerning profiling.

Who should use this guide?

This guide is primarily designed for those responsible for training law enforcement and border management officials. It may also directly support officers in mid-level positions to implement profiling techniques lawfully. It aims to increase understanding of the theory and practice of profiling, and to illustrate in concrete terms how profiling can be conducted in compliance with fundamental rights.

The guide covers profiling by frontline police officers – for example, during stop and search actions – and checks by border guards at border crossing points, namely

when a decision is taken to refer a person for a more thorough 'second line' check. In border management, it is a training aid for those teaching the common core curriculum of border-guard training under Article 36 (5) of the European Border and Coast Guard Regulation (Regulation (EU) No 2016/1624).

The guide also addresses profiling based on the analysis of large-scale data sets, including those regulated by EU law. Profiling in other situations, such as profiling carried out in the private sector for commercial purposes, is beyond the scope of this current guide. FRA is conducting further research on this topic.[2]

How to use this guide

This guide provides an overview of the main principles and practice of profiling in the context of law enforcement and border management. It can be read as a whole, or used as a reference to support training activities.

The guide contains three chapters. Chapter 1 explains the concept of profiling, clarifies when profiling becomes unlawful and describes its possible negative impact on individuals, communities, and on the exercise of police and border management powers. Chapter 2 details the principles and practices that should guide law enforcement officers and border guards implementing lawful profiling activities. Finally, Chapter 3 focuses on algorithmic profiling. Given that practice in this area is not so developed, this section contains fewer concrete examples. Instead it presents the principal risks to fundamental rights associated with computer-based profiling, and sets out the main legal requirements established by the General Data Protection Regulation (GDPR) and the Police Directive.

A number of visual elements highlight the different aspects of the guide. Key points summarise the main messages and are highlighted in yellow boxes. Light blue boxes highlight core aspects of the legal framework and green boxes present practical examples. Other boxes highlight important points to focus on, case studies, and caw law examples. Despite efforts to diversify the case studies, a disproportionate number of examples come from the United Kingdom (UK). This is because the UK has been addressing unlawful profiling since the 1980s, while other Member States have recognised unlawful profiling practices more recently. This means that the UK has developed more extensive and long-standing policies and practices in the field from which to draw examples.

---

2   See FRA's project on Artificial Intelligence, Big Data and Fundamental Rights.

How was the guide developed?

FRA organised a meeting with experts from various fields to discuss an early draft of the guide and to assist it in producing the final product.

In this respect, FRA would like to express its thanks to experts from the Office of the United Nations High Commissioner for Human Rights (OHCHR), the European Border and Coast Guard Agency (FRONTEX), the Office of Democratic Institutions and Human Rights (ODIHR) at the Organization for Security and Cooperation in Europe (OSCE), Amnesty International, the European Network Against Racism (ENAR), the International Centre for Migration Policy Development (ICMPD), the FIZ Karlsruhe, Leibniz Institut für Informationsinfrastruktur GmbH, European Digital Rights, Open Society Initiative for Europe, and representatives of the French Ombudsman, from the Dutch, Danish and Austrian police forces, and from the Polish Border Guards for their valuable feedback during the drafting of the guide.

Summary of the main points

1. Protected characteristics can never be the sole basis for profiling

- Profiling involves **categorising individuals** according to their characteristics.

- To collect and process **personal data**, law enforcement and border management authorities must ensure that data collection and processing have a legal basis, have a valid, legitimate aim, and are necessary and proportionate.

- **Protected characteristics** such as race, ethnic origin, gender or religion can be among the factors that law enforcement authorities and border guards take into account for exercising their powers, but they **cannot be the sole or main reason to single out an individual**. (For more information on 'protected characteristics', see Section 1.2.1.).

- Profiling that is based solely or mainly on one or more protected characteristics amounts to direct discrimination, and therefore **violates the individual's rights and freedoms** and is **unlawful**.

2. Any encounter with individuals should be respectful, professional and informative

- A **good quality encounter** in itself does not eliminate bias-based profiling, but is more likely to make the encounter more successful and reduce the possible negative impact of being stopped by a police officer or border guard. In border management, professional and respectful conduct is specifically referred to as a legal obligation.

- **Professional and respectful conduct** generally increases a person's satisfaction with the encounter.

- **Explaining the reasons for stopping** a person helps to boost public confidence in police and border management operations, and reduces the perception of bias-based profiling.

- Respect and politeness, however, **never justify unlawful border checks or stop and search actions**.

3. Profiling should be based on objective and reasonable grounds

- To be lawful, stops and referrals to second-line border checks must **be based on reasonable and objective grounds** of suspicion.

- Personal characteristics can be used as legitimate factors for profiling. However, to avoid being discriminatory, **there must *also* be reasonable grounds for suspicion** based on information other than protected characteristics.

- Law enforcement and border management actions based on **specific and up-to-date intelligence** are more likely to be **objective**.

- What is crucial is that a decision to stop an individual or refer them to a second-line border check should **not be based solely on an officer's *feeling*** about them, as this risks being based on bias, stereotypes and/or prejudice.

4. Unlawful profiling has a negative impact on policing and border management

- **Unlawful profiling undermines trust in the police and border guards**. It can cause a deterioration in the relationship between the police/border guards and members of minority and other communities who may feel singled out. This sense of injustice may lead to some individuals and groups losing trust in the police and other authorities, which may result in reduced reporting of crimes to the police and cooperation with the authorities. The authorities in turn may view certain groups with suspicion, which can trigger more unlawful profiling practices.

- **Unlawful profiling undermines the effectiveness of profiling**, as the rate at which individuals are stopped, either by police or at the border, does not necessarily correspond to offending rates among different groups.

- There is the risk of a **self-fulfilling prophecy** when a minority group is disproportionately targeted by police or border management officers, resulting in higher numbers of arrests or checks at the border.

5. Unlawful profiling has legal and financial consequences, and officers are accountable for it

- Law enforcement and border management officials are **accountable** for keeping profiling within the law.

- **Collecting reliable, accurate and timely data** is crucial for ensuring accountability.

- **Effective complaint mechanisms** can both deter abuses of power and help to secure and restore public trust in the operations of the police and border management authorities.

- **Feedback meetings with members of the public** (to listen to their opinions, discuss profiling, and gather feedback on operations, provide opportunities to learn important lessons and improve profiling actions.

6. Algorithmic profiling must respect specific data protection safeguards

- In developing and using algorithmic profiling, **bias** may be introduced at each step of the process. To avoid this and subsequent potential violations of fundamental rights, both the **IT experts and officers interpreting the data should have a clear understanding of fundamental rights**.

- Using **reliable data** is crucial. Entering data that reflect existing biases or come from unreliable sources into an algorithm will produce biased and unreliable outcomes.

- Algorithmic profiling must be **legitimate, necessary** and **proportionate.**

- Processing of data must have **a specific purpose.**

- Individuals have a **right to be informed,** by receiving information on the personal data that are collected and stored, on the processing and its purpose, and on their rights.

- Data should be **safely collected, processed and stored.** Authorities are expected to keep records of the processing activities (including what is done to the data) and of the logs relating to them (including information on the person/s accessing the data).

- Unlawful data processing must be **prevented and detected:** 1) through prior impact assessments, and 2) through the use of privacy tools embedded 'by design' in the algorithm.

Relevant websites

European Union
Court of Justice of the European Union (CJEU): http://www.curia.eu
EU legislation: http://eur-lex.europa.eu/
European Union Agency for Fundamental Rights (FRA): http://www.fra.europa.eu
European Parliament: http://www.europarl.europa.eu

Council of Europe
Committee of Ministers of the Council of Europe: http://www.coe.int/cm
European Court of Human Rights (ECtHR): http://www.echr.coe.int

United Nations
Office of the United Nations High Commissioner for Human Rights (OHCHR): http://www.ohchr.org

Fight against discrimination
European Commission against Racism and Intolerance (ECRI): http://www.coe.int/ecri
European Network of Equality Bodies (Equinet): http://www.equineteurope.org/
National Equality bodies: http://www.equineteurope.org/-Equinet-Members-

Data Protection
European Data Protection Supervisor (EDPS): https://edps.europa.eu/
European Data Protection Board (EDPB): https://edpb.europa.eu
National Data Protection Authorities: https://edpb.europa.eu/about-edpb/board/members_en

Law enforcement
Independent Police Complaints Authorities' Network (IPCAN): https://ipcan.org/
European Union Agency for Law Enforcement Training (CEPOL): https://www.cepol.europa.eu/
European Union Agency for Law Enforcement Cooperation (EUROPOL): https://www.europol.europa.eu/

Border management
European Border and Coast Guard Agency (FRONTEX): https://frontex.europa.eu/
European Asylum Support Office (EASO): https://www.easo.europa.eu/

Large-scale databases
European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA): https://www.eulisa.europa.eu/

1

Setting the scene:
What is profiling?

This chapter describes what is meant by profiling and explains the main fundamental rights it can affect. It introduces profiling in the context of law enforcement and border management activities by looking at three essential elements:

- The concept of profiling and its use by law enforcement and border management authorities. This section also introduces some of the different types of profiling.

- The most important fundamental rights principles that must be respected if profiling is to be conducted lawfully, namely non-discrimination and the rights to respect for private life and data protection.

- The potential negative impacts of profiling, including the possible consequences on individuals and on relationships with communities, and trust in the police and border management authorities.

1.1. Defining profiling

Profiling involves **categorising individuals** according to personal characteristics. These characteristics can be 'unchangeable' (such as age or height) or 'changeable' (such as clothing, habits, preferences and other elements of behaviour). Profiling includes data mining whereby individuals are categorised **"on the basis of some of their observable characteristics in order to infer, with a certain margin of error, others that are not observable"**.[3]

---

3   Dinant J.-M., Lazaro C., Poullet Y., Lefever N. and Rouvroy A. (2008), p. 3.

Key points

- Profiling involves **categorising individuals** according to their inferred characteristics.

- There are two main purposes of profiling in the context of law enforcement and border management: to **identify known individuals based on intelligence concerning a specific individual**, and as a **predictive method** to identify 'unknown' individuals who may be of interest to law enforcement and border management authorities. Both may include conscious or unconscious biases that may discriminate against individuals.

- Profiling activities of border guards and law enforcement officers may be influenced by biases originating either from their individual or institutional experiences. These biases may feed into and alter the profiling assessment, affecting both the lawfulness and effectiveness of policing.

- Stereotypes may reflect some statistical truth. However, even in these cases, they **remain problematic** if they result in an individual being treated as member of a group and not based on his/her individual situation.

- In developing and using algorithmic profiling, **bias may be introduced at each step of the process**. To avoid these and subsequent potential violations of fundamental rights, both the IT experts designing the algorithms and officers collecting and interpreting the data should have a clear understanding of fundamental rights and how to apply them in this context.

Profiling practices are used to:

- Generate knowledge, by analysing existing data to make assumptions about an individual. It uses past experiences and statistical analysis to establish correlations between certain characteristics and particular outcomes or behaviour.

- Support decision-making processes, by using these correlations to make decisions about what actions to take.

This makes profiling a powerful tool for law enforcement officers and border guards. However, it carries some significant risks:

- Profiling establishes general correlations that may not be true for each individual. Any given individual may be the 'exception to the rule'.

- Profiles may generate incorrect correlations, both for specific individuals and for groups.

- Profiles can create harmful stereotypes and lead to discrimination.

- Some stereotypes may reflect a statistical truth. However, even in these cases, stereotypes remain problematic if they result in a person being treated as a member of a group rather than as an individual.

> *Examples*
>
> *Potentially inaccurate profiling*
>
> *The assumption that 'women live longer than men' is underpinned by factual research; however, any particular man may live longer than any particular woman. Therefore, any decision-making towards woman based on this assumption carries the risk of being inaccurate in any single case and would only remain true only on average.*
>
> *Individuals may allow their family or friends to use their car, making unreliable any profile of risky driving behaviour based on ownership of the car.*

1.1.1. Profiling in the context of law enforcement and border management

Profiling is commonly, and legitimately, used by law enforcement officers and border guards to prevent, investigate and prosecute criminal offences, as well as to prevent and detect irregular immigration.

Profiling means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".[4] The results of this data processing are used to guide border management and law enforcement actions, such as stop

---

4 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, and repealing Council Framework Decision 2008/977/JHA, OJ L 119 (Police Directive), Art. 3(4).

and search, arrests, refusal of access to certain areas, or referral to more thorough 'second line checks' at the border. There are two main uses of profiling:

- To identify individuals based on specific intelligence. This uses a profile listing the characteristics of specific suspects, based on evidence gathered about a particular event.

- As a predictive method to identify 'unknown' individuals who may be of interest to law enforcement and border management authorities. This is based on data analysis and informed assumptions derived from experience. Ideally, predictive methods focus on behaviour. In practice, however, the focus is often not (or not only) on behaviour, but on visible physical characteristics, such as age, gender or ethnicity.

Table 1 presents a comparison of the key characteristics of these two types of profiling in the context of policing.

Table 1: Characteristics of specific intelligence-led policing and predictive policing

	Specific intelligence-led policing	Predictive policing
Context	A crime has been committed, or an alert has been issued on a specific person	No crime has been committed, or no alert has been issued on a specific person
Approach	Reactive	Proactive
Objective	To apprehend suspect(s)	To predict where and when crimes might happen or who might attempt to enter the country in an irregular manner
Data used	Specific intelligence related to the case (the 'individual profile')	Generic intelligence related to several cases
Type of process	Data-driven and human processes are combined	Mainly data-driven ('risk analysis')

Source: FRA, 2018

Both types of profiling can be unlawful if they are not done in accordance with specific safeguards, including having an objective and reasonable justification for the profiling. Chapter 2 and Chapter 3 provide practical information on how to ensure that profiling is both lawful and in accordance with human rights.

1.1.2. Defining algorithmic profiling

Rapid technological developments mean that profiling is increasingly based on the use of data stored in databases and information technology systems (IT-systems). Algorithmic profiling uses different techniques to profile people based on correlations and patterns in data. Algorithmic profiling allows law enforcement and border management officers to target individuals or specific groups that constitute a certain risk on the basis of data analysis.

Algorithmic profiling raises important fundamental rights issues, such as potential discrimination and violations of the rights to respect for private life and data protection. This section of the guide focuses on how law enforcement and border management officials can use and treat data in line with fundamental rights principles in their daily work.

Processing personal data: what does the law say?

The legal standards for processing personal data to construct profiles are set out in the EU's data protection legal framework. According to both Article 4 (4) of the General Data Protection Regulation (GDPR) and Article 3 (4) of the Police Directive, "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements".

Article 22 (1) of the GDPR states that profiling may only be accepted provided the decision is not solely based on automatic processing and does not produce effects on individuals that would significantly affect them.

Profiling falling under the scope of the Police Directive (see Section 3.1 on algorithmic profiling and data protection) should abide by Article 11 (3) of the Police Directive. It provides that "[p]rofiling that results in discrimination against natural persons on the basis of special categories of personal data referred to in Article 10* shall be prohibited, in accordance with Union law".

> * 'Special categories of personal data' are "personal data revealing racial or
> ethnic origin, political opinions, religious or philosophical beliefs, or trade
> union membership, and the processing of genetic data, biometric data
> for the purpose of uniquely identifying a natural person, data concerning
> health or data concerning a natural person's sex life or sexual orientation".
> *See* Police Directive, Article 10 (1).

The method used to generate profiles for algorithmic profiling is similar to a technique known as '**behavioural analysis**', where connections are made between certain characteristics and patterns of behaviour. Figure 1 shows how algorithms can be used to make predictions.

Focus on how algorithms are used to support decision-making

With the increased availability and use of data, decision-making is increasingly facilitated or replaced by predictive modelling methods, often referred to as the use of algorithms. An algorithm is a sequence of commands for a computer to transform an input into an output. Many algorithms are based on statistical methods, and use techniques which calculate relationships among different variables. For example, data on how much alcohol a group of people drinks and data on the life expectancy of the same group can be used together to calculate the average influence of drinking alcohol on life expectancy.

The output of algorithms is always a probability, which means that there is a degree of uncertainty about the relationships or classifications made. For example, email providers use algorithms to identify which messages are spam and send those to the junk mail folder. The algorithms work well, but are not perfect. Sometimes spam is not detected and ends up in the inbox; this is a false negative (i.e. it is falsely not identified as spam). Less often, a legitimate email might be picked out by the spam filter and sent to the junk mail folder; this is a false positive.

Having a basic understanding of how algorithms support decision-making allows practitioners to be able to identify and ask the right questions about potential problems with the use of algorithms, including their potential for discrimination and violations of the rights to respect for private life and data protection.

For more information, see FRA (2018b).

Figure 1: Algorithmic profiling process in the context of law enforcement and border management

Preparatory phase
- Design and development of the algorithm
- Specifying the goal of the analysis: prediction, description or explanation

Step 1
Data collection or selection of training data for predictive purposes
- Data are gathered by law enforcement agencies, border authorities and other public bodies. In some cases, the data may be purchased from private actors.
- Data are stored in warehouses, and prepared for analysis

Step 2
Data analysis /data mining
- The data are analysed to identify patterns and correlations.
- Statistical models are trained to set up a predictions

Step 3
Data interpretation or application of the predictive model
- The result of the analysis is used to identify behavioural patterns for given groups of individuals
- Decisions on law enforcement and broder management actions can be made on the basis of these profiles/predictions.

Source: FRA, 2018 (adapted from/based on Perry, W.L., et al. (2013), pp. 11–15, and Zarsky, T.Z. (2002–2003), pp. 6–18)

The creation of algorithms for prediction is a complex process that involves many decisions made by several people involved in the process. As such, it does not only refer to rules followed by a computer, but also to the process of collecting, preparing and analysing data. This is a human process that includes several stages, involving decisions by developers and managers. The statistical method is only part of the process for developing the final rules used for prediction, classification or decisions.[5] In any case, the way data are collected and used may be discriminatory.

---

5   FRA (2018b), p. 4.

> ***Example***
>
> *To be effective and accurate, facial recognition software needs to be fed with massive amounts of pictures and data. The more data it receives, the more accurate its findings will be. Yet to date, the images fed into algorithms to train them have largely been of white men, with comparatively low numbers of women and/or individuals of other ethnic backgrounds. As a result, the outputs produced by the software are less precise, and carry a greater likelihood of inaccuracy for individuals belonging to these groups. When used by law enforcement officers or border guards to profile people and decide on, for instance, their arrest, this can result in mistakes with a potentially serious impact on the rights and freedoms of the individual.*
>
> *For more information, see Center on Privacy and Technology at Georgetown Law (2016); and Buolamwini J., Gebru T. (2018).*

Bias may be introduced at each step of the process of algorithmic profiling. To avoid discriminatory bias and violations of the rights to data protection and privacy, both the people designing the algorithms and the law enforcement officers and border management officers collecting and interpreting the data should have a clear understanding of fundamental rights and their application in this context.

Using reliable data is crucial. In algorithmic profiling, the quality of the data used must be assessed to ensure it is reliable: the lower its variability, the higher its reliability. Using data which reflect existing biases or come from unreliable sources to build an algorithm will produce biased and unreliable outcomes. Errors might also occur during the predictions inferred from the data:

- False positives refer to cases where individuals are singled out and subjected to further scrutiny on the erroneous prediction that they constitute a risk.

- False negatives refer to individuals who pose a real risk in the context of law enforcement and border management operations but have not been identified as such by the system.

1.2.   When is profiling unlawful?

When used lawfully, profiling is a **legitimate investigation technique**. To be lawful, it must be based on **objective and reasonable justifications** and comply with fundamental rights, such as the right to non-discrimination and to protection of personal data. Profiling will be deemed to have no objective and reasonable justification "if it does not pursue a legitimate aim or if there is not a reasonable relationship of proportionality between the means employed and the aim sought to be realised".[6]

Profiling can touch on many different fundamental rights. This section focuses on the fundamental rights that are mainly affected by unlawful profiling: the right to non-discrimination, and the rights to privacy and data protection. Profiling will be deemed unlawful if:

- it includes acts of unjustified differential treatment of individuals on the basis of protected grounds (see Section 1.2.1), or

- it unnecessarily interferes with individuals' private lives, and/or is not in accordance with rules regarding the processing of personal data (see Section 1.2.2).

---

6   European Commission against Racism and Intolerance (ECRI) (2007), para. 28.

1.2.1.   The prohibition of discrimination

Prohibition of discrimination: what does the law say?

"**Any discrimination based on any ground** such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation **shall be prohibited**."*

Article 21 of the EU Charter of Fundamental Rights

"**The enjoyment of any right set forth by law shall be secured without discrimination on any ground** such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status. No one shall be discriminated against by any public authority on any ground such as those mentioned in paragraph 1."

Article 1 of the Protocol No 12 to the European Convention on Human Rights

* It should be noted that, in practice, many Member States have extended protection against discrimination beyond the grounds listed in the Charter and in the European Convention for Human Rights (ECHR).

Discrimination is "where one person is treated less favourably than another is, has been or would be, treated in a comparable situation" on the basis of a perceived or real personal characteristic.[7] These characteristics are called 'protected grounds' or 'protected characteristics' in non-discrimination law. More information on European law and jurisprudence in the area of non-discrimination is available in the 2018 edition of the Handbook on European non-discrimination, jointly published by FRA and the Council of Europe.[8]

---

7   Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, OJ L 180, Article 2; and Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ L 303, Art. 2.

8   FRA and Council of Europe (2018).

There are several types of discrimination:

Direct discrimination is when a person is treated less favourably, *solely or mainly* on the basis of a protected ground, such as race, gender, age, disability or ethnic origin.[9]

> **Example**
>
> *In response to a terrorist threat, the police are given the power to stop and search anybody they think might be involved in terrorism. The threat is believed to come from a terrorist organisation active in a certain region of the world, but there is no further specific intelligence. If a police officer stops a man solely or mainly because his appearance indicates that he may originate from the same region of the world, this would constitute direct discrimination and be unlawful.*

Indirect discrimination (also referred to as 'disparate impact discrimination' in the context of law enforcement and border management) occurs where an *apparently neutral* provision, criterion or practice would put persons having particular protected characteristics at a particular disadvantage compared to other persons, unless that provision, criterion or practice is objectively justified by a legitimate aim and the means of achieving that aim are necessary and proportionate.[10] Indirect discrimination generally requires statistics to assess whether an individual was, in practice, treated less favourably than another on the basis of their membership of a group with particular protected characteristics.

> **Example**
>
> *To perform routine controls, law enforcement authorities decide to stop one out of every 10 cars in town X between the hours of 21:00 and 01:00; 60% of the population of town X driving during these hours is of Afro-Caribbean descent, whereas the Afro-Caribbean population of the town and surrounding area does not exceed 30%. As this group is likely to be more negatively affected than others, it would amount to indirect discrimination.*

---

9   *Ibid.*, p. 43.

10   Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation, OJ L 303 (Employment Equality Directive), Art. 2; see also FRA and Council of Europe (2018), p. 53.

Addressing discrimination on the basis of a single ground fails to reflect adequately the various manifestations of unequal treatment. **Multiple discrimination** describes discrimination that takes place on the basis of several grounds operating separately. For instance, an individual may face discrimination not only because of their ethnic origin, but also their age and gender.[11] **Intersectional discrimination** describes a situation where several grounds operate and interact with each other at the same time in such a way that they are inseparable and produce specific types of discrimination (see Example box).

> **Example**
>
> *A police officer stops and searches a young man of African descent without reasonable suspicion that he has committed a crime. He is discriminated against not just because of his age – not all young people are stopped – or his ethnic origin – not all people of African descent are stopped, but precisely because he is both young and of African descent.*

Discrimination may also arise from the automated processing of personal data and the use of algorithmic profiling. Discrimination can occur during the design and implementation of algorithms, through biases that are incorporated – consciously or not – in the algorithm, as well as when decisions are made on the basis of the information obtained.

Article 9 (1) of the GDPR specifically states that the processing of special categories of personal data that reveal personal characteristics, such as racial or ethnic origin, political opinions, religious or philosophical beliefs shall be prohibited (see Figure 7 in Section 2.2.4 for the full list of protected grounds). This prohibition may be lifted in specific cases, such as the protection of public interest, providing that the exemption has a legal basis, is proportionate and necessary, and provides for adequate safeguards.[12]

Similarly, in the context of the prevention, investigation, detection and prosecution of criminal offences, Article 11 (3) of the Police Directive on automated individual decision-making prohibits "profiling that results in discrimination against natural persons on the basis of special categories of personal data", including data revealing

---

11   FRA and Council of Europe (2018), p. 59.

12   General Data Protection Regulation (GDPR), Art. 9(2)g.

racial or ethnic origin and religious beliefs, and genetic and biometric data.[13] Again, exceptions to this prohibition are permitted in certain cases, but must be necessary, have appropriate safeguards, and should either have a legal basis, or have the aim to protect the vital interests of an individual.[14]

Prohibition of discriminatory profiling: what does the law say?

"**Profiling that results in discrimination** against natural persons **on the basis of personal data** which are by their nature particularly sensitive in relation to fundamental rights and freedoms **should be prohibited** under the conditions laid down in Articles 21 and 52 of the Charter [of fundamental rights]."
Recital 38 of the Police Directive

"**Profiling that results in discrimination** against natural persons on the basis of special categories of personal data referred to in Article 10* **shall be prohibited**, in accordance with Union law."
Article 11(3) of the Police Directive

* Article 10 of the Police Directive: "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".

"While carrying out border checks, border guards **shall not discriminate** against persons on grounds of sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation."
Article 7 of the Schengen Borders Code

The prohibition of discrimination does not mean that personal characteristics cannot be used as legitimate factors for profiling in the context of criminal investigations or border checks (see Section 2.3). However, there must be reasonable grounds for suspicion based on information other than the protected grounds. For example, an

---

13   For more information see, Article 29 Data Protection Working Party (2017b).

14   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, and repealing Council Framework Decision 2008/977/JHA, OJ L 119 (Police Directive), Art. 10.

individual may match a specific description of a suspect, or their appearance may not correspond to the information contained in their travel document.[15]

Focus on discrimination on the grounds of nationality

Article 21 of the EU Charter of Fundamental Rights **limits the prohibition of discrimination on the grounds of nationality to EU citizens**. The Racial Equality Directive does not include nationality among the protected grounds.

However, Member States have broadened the scope of the prohibition of discrimination to cover nationality in various ways. This includes acknowledging that nationality is sometimes used as a proxy for race, ethnic origin, or religion. In certain such cases, "differences of treatment on grounds of nationality […] [will be] found in violation of legislation prohibiting discrimination on these grounds" (see European network of legal experts in gender equality and non-discrimination, 2016, p. 99). In practice, discrimination on the grounds of nationality and discrimination on the grounds of ethnicity are often difficult to distinguish.

The fact that nationality is not explicitly mentioned as a potential ground of discrimination in Article 21 of the Charter primarily reflects the different status of EU citizens (and other persons enjoying the right of free movement under EU law) and third-country nationals under EU law. This is of particular significance in border procedures, where nationality is the decisive factor in determining whether an individual will be subject to a thorough check, or must hold a visa to enter – or transit through – the Schengen area.

At the same time, a systematic referral to second line checks of all persons of a specific nationality risks becoming discriminatory. Nationality can be a legitimate part of risk profiles to detect irregular migration or presumed victims of trafficking in human beings, but must not be the sole or primary trigger of a second line check. Furthermore, as in other contexts, differential treatment based on nationality becomes discriminatory and therefore unlawful when it is used as a proxy for discriminating on protected grounds that are closely linked to nationality, such as race, ethnicity or religion.

---

15 United Kingdom, House of Lords (2006), Lord Scott, Opinions of the Lords of appeal for judgment in *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.,* [2006] UKHL 12, 8 March 2006, para. 67.

In its 2014 Recommended Principles and Guidelines on Human Rights at International Borders, the Office of the UN High Commissioner for Human Rights includes nationality among the protected grounds which should not be used for the profiling of migrants (Principle 8).

Case law

In *Rosalind Williams Lecraft v. Spain*, a woman was stopped by a police officer on the platform of a train station in Spain and asked to show her identity papers. The woman asked the police officer why she was the only person stopped on the platform and was told: "It's because you're black." In its ruling, the UN Human Rights Committee underlined that it is generally legitimate to carry out identity checks in the interest of public safety and to prevent crime and monitor irregular immigration. However, it found that "when the authorities carry out these checks, the physical or ethnic characteristics of the persons targeted should not be considered as indicative of their possibly illegal situation in the country. Nor should identity checks be carried out so that only people with certain physical characteristics or ethnic backgrounds are targeted. This would not only adversely affect the dignity of those affected, but also contribute to the spread of xenophobic attitudes among the general population; it would also be inconsistent with an effective policy to combat racial discrimination".

In 2017, a similar complaint was filed with the ECtHR, involving the treatment of a Pakistani national during and after a police stop in Spain. The court will have to decide whether the applicant suffered discrimination on the grounds of ethnic origin during the identity check, and whether there was a violation of Article 8 (right to private and family life) as regards the Spanish authorities' failure to take all reasonable steps to uncover any possible racist motives behind the incident. The judgment is pending at the time of writing.

For more information, see UNHRC, Rosalind Williams Lecraft v. Spain, Comm. No. 1493/2006 and ECtHR, Zeshan Muhammad v. Spain, No. 34085/17, lodged on 6 May 2017. See also FRA and Council of Europe (2018).

In *B.S. v. Spain,* a female sex worker of Nigerian origin, who was legally resident in Spain, alleged that the Spanish police mistreated her physically and verbally on the basis of her race, gender and profession. She claimed

that, unlike other sex workers of European origin, she was subject to repeated police checks and a victim of racist and sexist insults. Two third-party interventions from the AIRE Centre and the European Social Research Unit of the University of Barcelona asked the ECtHR to recognise intersectional discrimination. The court found a violation of Article 3 (prohibition of inhuman and degrading treatment), but went further to examine separately whether there was also a failure to investigate a possible causal link between the alleged racist attitudes and the violent acts of the police. On this issue, the ECtHR found a violation of Article 14 (prohibition of discrimination), because the domestic courts had failed to take into account the applicant's particular vulnerability as an African woman working as a prostitute. Although taking an intersectional approach, the judgment did not use the term 'intersectionality'.

For more information, see ECtHR, B.S. v. Spain, No. 47159/08, 24 July 2012.

Focus on the burden of proof

In 2016, the French Court of Cassation ruled for the first time on the question of discriminatory identity checks. In its *Decisions of 9 November 2016*, the court ruled that the police conducted discriminatory identity checks on three out of 13 men of African or Arab origin. It found that the state was responsible in these cases, and ordered it to pay compensation to the three claimants. In eight other cases, the court ruled that the contested identity checks were legal, as they were based on objective and therefore non-discriminatory elements. The judges did not rule on the two other cases, sending them back to the lower courts for retrial.

The court also clarified the burden of proof in such cases. Identity checks are not recorded when they do not lead to judicial or administrative proceedings. The court explained that claimants should provide courts with evidence to indicate the existence of discrimination. The police must prove either the absence of differential treatment in the implementation of identity checks, or that the differential treatment was justified by objective elements.

Moreover, the court found that judges can take into account, as evidence, studies and statistical information attesting to the frequency of identity checks carried out, on discriminatory grounds, on the same population group as the claimant (i.e. visible minorities, as determined by physical

characteristics resulting from real or supposed ethnic origin). However, this evidence alone is insufficient to suggest discrimination.

Therefore, the court held that an identity check based on physical characteristics associated with an actual or supposed ethnic origin, without any prior objective justification, is discriminatory and represents serious misconduct which, in these three cases, involved the responsibility of the state.

For more information, see France, Court of Cassation (Cour de Cassation), Décision 1245, 9 November 2016.

1.2.2. The right to respect for private life and the protection of personal data

Under EU law, the right to respect for private life (Article 7 of the Charter) and the protection of personal data (Article 8 of the Charter) are distinct, albeit closely related rights. The right to private life (or right to privacy) is a broader right, which prohibits *any interference* in the private life of an individual. Private life is under-stood not simply as what one wishes to keep confidential, but also as the means through which one expresses one's personality, for instance by choosing whom to interact with or how to dress. The protection of personal data is limited to the assessment of the lawfulness in relation to the *processing of personal data*.[16] When not referring specifically to EU law, the two are used interchangeably for the purpose of this guide. These rights are not absolute and can be limited in certain circumstances (see Article 8 of the ECHR and Article 52 of the Charter).

Rights to privacy and protection of personal data: what does the law say?

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime,

---

16   FRA, EDPS and Council of Europe (2018).

for the protection of health or morals, or for the protection of the rights and freedoms of others."

Article 8 of the European Convention on Human Rights

"Everyone has the right to respect for his or her private and family life, home and communications."

Article 7 of the EU Charter of Fundamental Rights

"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. (...)"

Article 8 of the EU Charter of Fundamental Rights

"1. The data subject shall have the right not to be subject to a decision **based solely on automated processing**, including profiling, which **produces legal effects** concerning him or her **or** similarly **significantly affects him or her**.

2. Paragraph 1 shall not apply if the decision:

a) is necessary for entering into, or the performance of, a contract [...];

b) is authorised by [...] law [...] which lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c) is based on the data subject's explicit consent.

Article 22(1) and (2) of the General Data Protection Regulation

"Member States shall provide for a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects him or her, to be prohibited unless authorised by Union or Member State law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention on the part of the controller."

Article 11(1) of the Police Directive

EU secondary law elaborates on the rights to privacy and the protection of personal data. Two pieces of legislation specify how personal data can be collected and processed. Regulation 2016/679, the General Data Protection Regulation (GDPR), sets out general principles and safeguards concerning the processing of personal data. More specifically, Directive 2016/680, known as the Police Directive, sets the rules for the processing of personal data in the context of law enforcement operations

Table 2: Data protection requirements - differences between the Police Directive and the GDPR

Data protection principle	GDPR	Police Directive
Lawfulness, Fairness, Transparency	Personal data must be processed fairly, lawfully, **and in a transparent manner**.	Personal data must be processed fairly and lawfully.
Purpose limitation	Personal data collected for one purpose should not be further processed for an incompatible purpose; **further processing for scientific, historical or statistical purposes shall not be incompatible with initial purposes**	Personal data collected for one purpose should not be subsequently processed for an incompatible purpose; Other purposes shall not be incompatible with the initial purpose if such processing is authorised by law and is necessary and proportionate.
Data minimisation	Personal data collected shall be adequate, relevant **and limited to what is necessary** in relation to the purposes for which they were collected;	Personal data collected shall be adequate, relevant and **not excessive** in relation to the purposes for which they were collected.
Storage limitation	Personal data should be kept in a form which permits identification of data subjects for the period necessary to fulfil the purpose for which those data were collected; **personal data may be stored for longer periods for scientific, historical or statistical purposes.**	Personal data should be kept in a form which permits identification of data subjects, for the period necessary to fulfil the purpose for which those data were collected.
Accuracy	The personal data collected should be accurate and up to date. Incorrect or inaccurate personal data should be erased or rectified.	
Integrity and confidentiality	Personal data should be kept secure against unauthorised or unlawful processing and against accidental loss, destruction or damage.	

Source: FRA, 2018

for the purposes of prevention, investigation, detection or prosecution of criminal offences. The most important principles and some key differences between the two are illustrated in Table 2. The laws setting up the large EU databases used for border management, such as the Visa Information System (VIS), the Entry/Exit System (EES) or the European Travel Information Authorisation System (ETIAS), also each contain a dedicated data protection framework (see Section 3.2 on large-scale databases).

Examples

A border guard sends the list of passengers on a plane to unauthorised persons. Once shared, these personal data may be used for other and/or private purposes. This is a clear breach of data protection principles.

A police officer leaves her office with a list of personal data related to suspects on her computer screen. By undermining the principle of security of personal data, this constitutes a violation of data protection principles.

Case Law

Court judgments give guidance on how these principles are applied in practice.

Purpose limitation

In *Heinz Huber v. Bundesrepublik Deutschland,* the CJEU assessed the legitimacy of the German Central Register for Foreign Nationals (*Auslanderzentralregister, AZR*) which contains certain personal data relating to foreign nationals – both EU and non-EU citizens – who reside in Germany for more than three months. The CJEU concluded that data collected for a specific purpose cannot be used for a different purpose. The court considered that the AZR is a legitimate instrument to apply residence rules, and that the difference in treatment between foreign nationals and German nationals, on whom less data is kept, is justified given the intended purpose. However, the CJEU found that data stored in the AZR cannot be used for fighting crime in general, as this is a different purpose from that for which the data were originally collected.

For more information, see CJEU, Case C-524/06, Heinz Huber v. Bundesrepublik Deutschland*, 16 December 2008.*

Storage limitation

In *S. and Marper v. United Kingdom,* the applicants asked for the deletion of their records (fingerprints, cellular samples, and DNA profiles) from the DNA database used for criminal identification in the United Kingdom. Their trials had ended in acquittal and they were concerned about possible current and future uses of their data. The police refused. The ECtHR concluded that holding indefinitely the DNA samples of individuals who are arrested but later acquitted or have the charges against them dropped, is a violation of the right to privacy. The court highlighted the risk of stigmatisation, as the data of people who had not been convicted of any offence were treated in the same way as that of convicted persons. The court also recognised that the potential harm caused by retention of these data is particularly significant in the case of children, given the importance of their development and integration in society.

For more information, see ECtHR, S. and Marper v. United Kingdom*, Nos. 30562/04 and 30566/04, 4 December 2008.*

To collect and process personal data for the purposes of profiling, law enforcement and border management authorities must meet four essential legal criteria. The collection and processing of data must:

• **be defined and regulated by law (*legal basis*)**: any limitation of the rights to respect for private life and data protection must be stipulated by law and respect the essence of those rights. The law must meet the standards of clarity and quality, meaning that the public have access to it and it is sufficiently clear and precise for the public to understand its application and consequences;

• **have a valid, lawful and appropriate purpose (*legitimate aim*):** legitimate aims are set out in law and cannot be extended further. They may relate to national security, health, public order, or crime prevention;

• **be indispensable to achieving this purpose (*necessity*):** the processing of personal data should be limited to what is necessary for the purpose for which the data were collected;

- **not be excessive (*proportionality*):** authorities processing personal data should achieve a fair balance between the purpose and the means used to achieve it. In other words, the added value of the processing should not outweigh its potential negative impact.

Chapter 3 explains how these principles can be applied in practice.

Figure 2 shows how these principles can be used to assess whether an action might infringe the rights to respect for private and family life and data protection (see also Section 2.3.3 on complaints mechanisms). The stop and search case of *Gillan and Quinton v. the United Kingdom* illustrates how the ECtHR applied these principles to determine whether there had been an infringement of the right to data protection and privacy (see box on Case law).

Figure 2:   Infringement of privacy and data protection – the assessment process

Source: FRA, 2018 (based on Council of Europe (2003), The right to respect for private and family life: A guide to the implementation of Article 8 of the European Convention on Human rights)

Case law

In *Gillan and Quinton v. the United Kingdom*, the applicants, two British nationals, sought to challenge the legality of stop and search powers used against them by way of judicial review.

Is the measure adopted prescribed by law? The measure was in accordance with Sections 44–47 of the Terrorism Act 2000, which established that: 1) for the prevention of acts of terrorism, senior police officers could authorise any uniformed police officer in a given area to conduct stop and search actions; 2) authorisations were subject to confirmation by the Secretary of State and were time bound, but could be renewed indefinitely; 3) although the purpose of such search operations was to find items that could be used for acts of terrorism, stop and search actions did not have to be based on a suspicion that the person(s) stopped was carrying items of that kind; and 4) people refusing to undergo a search operation were liable to imprisonment, a fine, or both (*Gillan and Quinton*, para. 76-80).

Does the measure adopted interfere with privacy and/or data protection? The use of coercive powers by law enforcement authorities to stop a person and search their clothing and belongings represents a clear interference with the right to respect for private life. Its seriousness is amplified by the public exposure of personal information, which entails an element of humiliation and embarrassment (*Gillan and Quinton*, para. 63).

Assessment of proportionality and necessity: The court expressed a number of concerns about the proportionality and necessity of the law (*Gillan and Quinton*, para. 80-86):

- the statutory standard for the authorisation of stops was not burdensome;

- the breadth of the statutory powers is such that individuals face formidable obstacles in showing that any authorisation and confirmation is beyond the powers of the relevant authorities (*ultra vires*) or an abuse of power;

- the geographical areas covered by the authorisation were very broad and the time limit was repeatedly extended, reducing the targeted nature of the authorisation;

- restrictions on the discretion of individual officers were more formal than substantial;

- there was little prospect of judicial remedy because the officer conducting the stop did not have to demonstrate the reasonableness of their suspicion; proving that the power had been improperly exercised was therefore almost impossible.

These considerations led the ECtHR to conclude that the relevant sections of the Terrorism Act were "neither sufficiently circumscribed nor subject to adequate legal safeguards against abuse", and therefore violated Article 8 of the ECHR.

For more information, see ECtHR, Gillan and Quinton v. the United Kingdom, *No. 4158/05, 12 January 2010.*

The legal requirements concerning profiling set out in the reformed EU data protection legal framework are detailed in Chapter 3.

1.3. What are the potential negative impacts of unlawful profiling for law enforcement and border management?

Profiling based only on broad categories, such as race, ethnic origin or religion, is not only unlawful but may also have disadvantages for effective policing and border management authorities. This section looks at two potential negative impacts:

- The greatest difficulty relates to the strain it can place on relations with communities. Profiling can generate resentment among the communities particularly affected, and reduce trust in the police and border management authorities. This in turn can undermine the effectiveness of methods that rely on public cooperation.

- There are also doubts about the effectiveness of using broad categories of profiles in border management or law enforcement, for instance if it results in an individual being falsely placed under suspicion.[17]

---

17   FRA (2017d), p. 51.

In addition, where profiling is conducted in an unlawful manner, authorities will be open to complaints procedures or legal action. This can take the form of internal supervision through police complaints authorities, specialised complaints bodies, supervisory authorities, or the civil and criminal court system (see Section 2.3). Individual officers and mid-level managers may be subject to administrative and/or criminal sanctions as a result of their involvement in, or acquiescence to, unlawful profiling. This can place a drain on resources, as well as damaging authorities' morale and reputation.

Key points

- **Unlawful profiling undermines trust** in law enforcement and border management authorities, and can result in a deterioration in relations with local communities.

- There are **doubts about the actual effectiveness of using broad profiling** to detect crime or in border management. Evidence is inconclusive about whether such profiling increases the success rate of law enforcement or border management operations.

1.3.1. Impact on trust in the police and border management and good community relations

Research shows the negative impact the use of broad profiles can have on the individuals targeted and the communities to which they belong.[18] The box below captures some individuals' responses after being subject to a stop and search or border check.

> *Examples*
>
> *Impact of stop and search actions and border checks on individuals*
>
> *1. Police stops – Keskinen, S. et al (2018)*
>
> *Between 2015 and 2017, the Swedish School of Social Science at the University of Helsinki interviewed 185 people about their experiences of ethnic profiling. The research indicated that most respondents found stops*

---

18   FRA (2017d).

to be unpleasant, annoying or humiliating experiences. Below are some extracts of respondents' testimonies.

"Then somewhat later, another police stopped me again [...] while I was walking along the street with two white friends: one Finnish and the other Dutch. And did exactly the same thing ... asking about the same question. I was pissed off because I did not know why I was being singled out. I asked them and they just claimed they are doing their job." (Female, 30s, African country)

"Once my mum and my brother were outside walking in town and then the policemen stopped them and they said 'Show us your passports'. And I consider that ethnic profiling. And then my brother [said in Finnish] 'We don't have our passports we don't carry them all the time'. And then once they saw that he speaks fluent Finnish they were like 'Oh never mind'. I was angry because I know ethnic profiling is illegal and my mom and my brother [they] didn't know. So I felt like, you know, they were mistreated. So I was very angry. Once I told them that it's illegal what happened to them like obviously they knew that they got stopped because they [...] were not Finnish-looking, they were foreign-looking." (Female, 20s, Somalia-Finland)

"They always have a similar description all the time. It makes me wonder, so for 11 years they've been looking for the same person who managed to elude you guys, you're not doing a good job then, because the description they [border control] have is always similar, and I always match that description [laughter]." (Male, early 30s, African country-Finland)

For further information, see Keskinen, S. et al (2018), The Stopped – Ethnic Profiling in Finland.

2. Border checks – FRA (2014a and 2014b)

"I understand why [the border guard] stopped me but he didn't have to send me here [second line check/police station], or treat me like a criminal. They do this with all Eastern Europeans".
(Passenger from Serbia, male, interviewed at Frankfurt airport)

Question:*"How do you think the treatment was at the first-line check?"*

Reply:*"I think it was not good. It was humiliating. He treated me badly. He just took my passport, looked at it and then just called immigration. He asked some questions and raised his voice, but I didn't understand anything. They took me out of the line but they did not respect me and they made me scared."*

Q:*"Why did you feel scared or humiliated?"*

R:*"Because I didn't know what was going to happen and they couldn't explain anything. And a lot of people were around and the guard talked with the other guards without talking to me. Then I had to wait and I still didn't know why I was there."*
(Passenger from Angola, male, interviewed at Schiphol)

"I really understand the […] border guards. For them too, it is really difficult to work at the booths hours and hours! So, from time to time, they show negative attitudes, such as shouting, to people like us." (Male, Turkish national, truck driver frequently crossing the border, Kipi)

The sum of these individual experiences may translate into negative group effects.[19] This can contribute to a marked deterioration in the relationship between the police and border management officials and members of minority communities subject to high levels of stop and search actions or enhanced border checks.

Case study

The role of stop and search in public disorder (UK 2011 and France 2005)

Following riots in several major UK cities during August 2011, the London School of Economics and the Guardian newspaper interviewed 270 rioters about why they had participated in the riots. The study found that distrust and antipathy towards the police was a significant factor, and that "[t]he most common complaints related to people's everyday experience of policing, with many expressing deep frustration at the way people in their communities were subjected to stop and search" actions.

For more information, see London School of Economics (2011).

---

19   United Nations (UN) (2007), para. 57.

Similar dynamics were identified in other EU Member States. In France, riots in November 2005 were found to be triggered by an event involving the accidental death of two minority youths while allegedly being pursued by the police (see Jobard, 2008, and Body-Gendrot, 2016).

For more information, see Hörnqvist (2016).

Linked to this, profiling can result in increased levels of hostility in other encounters between individuals and the police or other law enforcement bodies. Greater hostility increases the chances that routine encounters will escalate into aggression and conflict, posing safety concerns for officers and community members alike.

More broadly, recent research shows that being stopped, arrested, convicted, or jailed tends to keep people away from other public services beyond the criminal justice system, such as health, employment, and educational organisations.[20] Without undermining the legitimate reasons that lead to the arrest of convicted individuals, it should be borne in mind that the exclusion of already marginalised segments of the population from such institutions can undermine social inclusion and integration of minority groups.

Focus on FRA's EU-MIDIS II findings

In 2015 and 2016, FRA collected information from over 25,500 respondents with different ethnic minority and immigrant backgrounds across the 28 EU Member States.

What information was collected?

In relation to profiling, respondents were asked if they thought that they had been stopped by the police because of their immigrant or ethnic minority background and about the way they were treated by the police, including any experiences of physical assault by the police. The survey did not ask about encounters with border management

---

20   Brayne, S. (2014), pp. 367–391.

Figure 3: Most recent police stops perceived as ethnic profiling among those stopped in the five years before the EU-MIDIS II survey, by EU Member State and target group (%) [a,b,c,d]

SSAFR
- FI 27
- IE 28
- PT 35
- UK 38
- LU 40
- FR 42
- DE 42
- DK 47
- SE 51
- AT 56
- IT 60
- MT 66
- Group average **41**

TUR
- AT 14
- DE 16
- DK 17
- BE 23
- SE 31
- NL 43
- Group average **17**

NOAFR
- FR 33
- ES 47
- BE 52
- NL 61
- IT 71
- Group average **38**

(S)ASIA
- CY 43
- UK 45
- IT 46
- EL 89
- Group average **47**

RIMGR
- SI 5
- PL 9
- Group average **6**

ROMA
- BG 19
- HU 27
- SK 35
- HR 45
- ES 46
- RO 52
- CZ 57
- EL 63
- PT 84
- Group average **42**

RUSMIN
- LV 0
- LT 0
- EE 0
- Group average **0**

TOTAL EU-28 42

Notes:
[a] Out of respondents who were stopped by the police in the five years before the survey (n=6,787); weighted results.

[b] Results based on a small number of responses are statistically less reliable. Thus, results based on 20 to 49 unweighted observations in a group total or based on cells with fewer than 20 unweighted observations are noted in parentheses. Results based on fewer than 20 unweighted observations in a group total are not published.

[c] *Questions: "In the past five years in [COUNTRY] (or since you have been in [COUNTRY]), have you ever been stopped, searched or questioned by the police?"; "Do you think that THE LAST TIME you were stopped was because of your ethnic or immigrant background?"*

[d] *Acronyms for target groups refer to immigrants from [country/region] and their descendants: TUR = Turkey, SSAFR = Sub-Saharan Africa, NOAFR = North Africa, SASIA = South Asia, ASIA = Asia, ROMA = Roma minority.*

Source: FRA, 2017b

What do the results show?

<u>Stops and ethnic origin</u>: The results show that 26 % of all EU-MIDIS II respondents were stopped by the police in the five years before the survey. Of those stopped in the five years before the survey, 33 % said that this was because of their ethnic and immigrant background.

<u>Perception of discrimination</u>: On average, nearly every second respondent with Asian (47 %), Sub-Saharan (41 %) and North African (38 %) backgrounds who was stopped during this timeframe said they were stopped because of their immigrant or ethnic minority background. Similarly, among stopped Roma respondents, nearly every second person (42 %) believed this was because of their ethnic background. By contrast, this percentage is much lower among the stopped respondents with Turkish background (17 %) (see Figure 3).

<u>Respect</u>: The findings show that a majority (59 %) of all respondents who were stopped by the police in the five years before the survey felt that they were treated respectfully (25 % 'very respectful', 34 % 'fairly respectful'). One in four (24 %) said that the way the police treated them was 'neither respectful, nor disrespectful'. Meanwhile, 17 % said that the police treated them disrespectfully (8 % 'fairly disrespectfully' and 9 % 'very disrespectfully'). Roma respondents and respondents with a North African background who were stopped indicated experiencing disrespectful behaviour by police during the most recent stop (25 % and 21 %, respectively) more often than other target groups.

For more information, see FRA (2017b).

Focus on the importance and usefulness of collecting data on police stops

Of the 28 EU Member States, the United Kingdom is currently the only one where data collection on police stops systematically includes information on the ethnicity of those stopped (see also Section 2.2.5. and Section 2.3.1.).

The data collected measure the 'stop and search rate' for different ethnic groups in England and Wales. The ethnic categories used are those listed in the UK Census from 2001. This census identified 16 categories, which were merged into five broader groups:

- White: English/Welsh/Scottish/Northern Irish/British; Irish; and any other White background.
- Mixed/Multiple ethnic groups: White and Black Caribbean; White and Black African; White and Asian; and any other Mixed/Multiple ethnic background.
- Asian/Asian British: Indian; Pakistani; Bangladeshi; and any other Asian background.
- Black/African/Caribbean/Black British: African; Caribbean; and any other Black/ African/ Caribbean background.
- Other ethnic groups: Chinese; and other ethnic groups.

The stop and search data collected compare the number of people stopped and searched from a particular ethnic group with the total number of people from that ethnic group living in the area, and then calculates a rate per 1,000 people.

For 2016-2017, the analysis of the data collected shows that there were four stops for every 1,000 White people, compared with 29 stops for every 1,000 Black people. The data also indicate that the highest rates were found among the three Black ethnic groups - Other Black (70 stops per 1,000 people), Black Caribbean (28 per 1,000 people) and Black African (19 per 1,000 people).

Without evidence provided by disaggregated data, it is difficult to prove whether there are differences in police action towards particular ethnic groups and – if this is the case – whether these differences might be the result of discriminatory profiling practices. Disaggregated data are available in the public domain in England and Wales, broken down by police force. This

allows for the identification of differential practices between forces that either can be explained as legitimate, or which might be used to identify potential discrimination in policing practices. Data are also used at the level of individual police officers to identify discriminatory practices in their work.

For more information, see Gov.uk's webpage on stop and search*, the Independent Office for Police Conduct's* website *and the Home Office's* website on open data about crime and policing*. See also United Kingdom (2018). For guidance on recording methodologies, see Open Society Justice Initiative (2018b).*

Case study

Survey on relations between the police and the public in France

In 2016, the French Ombudsman (*Défenseur des droits)* conducted a survey on Access to Rights. The *Défenseur des droits* also acts as the national police complaints commission. The survey covered a representative sample of more than 5,000 people.

The first part of the report presents the results related to the behaviour of law enforcement authorities. Overall, the survey indicates good relations between the public and the police. The vast majority of respondents said they trust the police (82 %).

Looking specifically at identify checks, the survey shows that most people do not experience identity checks: 84 % of respondents said they have not been checked in the last five years (90 % of women and 77 % of men). Those who said they had been checked generally report low instances of behaviour breaching the security forces' professional ethics during the most recent identify check, such as informal modes of address (16 %), brutality (8 %) or insults (7 %). However, 29 % reported a lack of politeness, and more than half of the respondents (59 %) who had been checked mentioned that the reasons for the check had not been explained. Generally, identity checks are perceived as being more legitimate when the security forces take the time to explain the reasons for the check.

The data also reveal that specific groups of people report more negative experiences. Young men aged 18-24 are nearly seven times more likely to experience frequent identity checks (i.e. more than five times in the last five years) than the general population, and men perceived as Black or Arab are between six and 11 times more affected by frequent identity checks than the rest of the male population. If we combine these two criteria, 80 % of men under the age of 25, and perceived as Arab or Black, have been checked at least once in the last five years (compared to 16 % of other respondents). Compared to the general population, this group is 20 times more likely to be subject to identity checks.

In addition, young men perceived as Black or Arab reported higher levels of problematic behaviour during the most recent identity check, such as using informal modes of address (40 % against 16 % of the total sample), insults (21 % against 7 % of the total sample), or brutality (20 % against 8 % of the total sample). These negative experiences and the frequency of checks are associated with a low level of trust in the police. Indeed, this group reported deteriorating relations with the police.

Finally, the results show that few respondents (5 %) who indicate breaches of professional ethics during identity checks take steps to report this situation. They mainly indicate that they do not report their experiences because these steps are considered as useless.

For more information, see Défenseur des droits (2017).

Where broad profiles are applied to a minority group, it, in conjunction with other stigmatising policy actions, may lead this group to develop a negative perception of itself. In addition, the wider community may develop a negative perception of that group. The minority group may become a "suspect community", associated by the public with criminality.[21] This may result in increasing prejudice.

---

21   European Monitoring Centre on Racism and Xenophobia (2006), p. 54.

The minority group may become targeted by a disproportionate amount of police resources which, in turn, is likely to lead to higher numbers of arrests or checks at the border. As a result, a self-fulfilling relationship between intensive policing and higher arrest rates can be established (see box).[22]

Focus on the risk of a 'self-fulfilling prophecy'

When police officers base their profiling not on reasonable grounds but on prejudices, they are likely to interpret information in a way that confirms their own biases. This is called a 'confirmation bias'. This happens when police officers' prejudices mean that they expect an individual to act unlawfully based on the person's actual or perceived race, ethnic origin, gender, sexual orientation, religion, or other protected ground. Because of this kind of bias, officers with such prejudices are likely to single out more individuals matching this description.

Since it is more likely that evidence of criminality will be found among individuals who are stopped than those who are not stopped, this bias-based profiling reinforces an officer's existing stereotypes. This false 'proof' that the decision to stop these individuals was correct is called a 'self-fulfilling prophecy'. Such bias-based profiling is discriminatory, unlawful, ineffective, and perpetuates stereotypes.

Figure 4 describes how the 'self-fulfilling prophecy' perpetuates the criminalisation of individuals.

---

22   Harcourt, B. (2004), p. 1329-1330; House of Commons Home Affairs Committee (2009), para. 16; and UN (2007).

Figure 4: The cycle of the self-fulfilling prophecy

Some of the members of that ethnic group stopped are indeed acting unlawfully

Individuals to be stopped only because they are or perceived to be of one ethnic group

Personal or institutional bias that persons belonging to a specific ethnic group are criminals

Stopping people from this ethnic group is falsely perceived as effective

Self-fulfilling prophecy perpetuating discrimination

Source: FRA, 2018

1.3.2. The effectiveness of profiling

There are also doubts about the effectiveness of using profiling based on broad categories to detect crime. It is unclear whether profiling actually increases the success rate (or 'hit rate') of law enforcement operations.

Some evidence suggests that the rates at which individuals are stopped does not necessarily correspond to offending rates among different ethnic or racial groups (see box). It should be noted that criminal justice data in most EU Member States do not allow for an overview of the progress of an individual case through the criminal justice system. As such, it cannot be determined whether an arrest results in prosecution and sentencing.

Case study

Changed search patterns lead to a higher 'hit rate' (1998-2000, USA)

In 1998, 43 % of the searches US Customs performed were on Black and Latino people, a far higher rate than their proportion among travellers. A particularly large number of searches, including invasive x-rays and strip

searches, were carried out on Latina and Black women suspected of being 'drug mules'. This was based on a profile that relied heavily on nationality and ethnicity. The hit rates for these searches were low across all groups: 5.8 % for 'whites', 5.9 % for 'blacks' and 1.4 % for 'Latinos'. It was particularly low for 'Latina' women, who were in fact the least likely to be carrying drugs on or in their bodies. In 1999, US Customs changed its procedures, removing race from the factors to consider when making stops. Instead, observational techniques focusing on behaviour such as nervousness and inconsistencies in passenger explanations, more intelligence information, and closer supervision of stop and search decisions were introduced. By 2000, the racial disparities in customs searches had nearly disappeared. The number of searches carried out dropped by 75 % and the hit rate improved from just under 5 % to over 13 %, and became almost even for all ethnic groups.

For more information, see Harris (2002), USA (2000).

Ineffectiveness of unlawful profiling (2007-2008, Hungary)

Research conducted in Hungary showed that Roma people were disproportionately targeted for identity checks. About 22 % of all people checked by the police belonged to the Roma community, when the proportion of Roma people in the population was around 6 %. The disproportionately high number of identity checks on Roma people was not reflected in evidence of unlawful behaviour: 78 % of identity checks involving Roma individuals resulted in no action taken by the police, and 19 % were linked to a petty offence* (compared to 18 % of checks on the general population). In addition, the arrest rates for the Roma community and the general population were similar.

For more information, see Tóth, B.M. and Kádár, A. (2011).

* "Petty offences are quasi-criminal offences, the gravity of which does not reach the criminal level (i.e. they are not regulated in the Criminal Code). Petty offences range between offences that are punishable by a 60-day incarceration, such as prostitution or physical threats, to those punishable by less severe measures (e.g. a fine, confiscation of goods, or ban on entering certain events). Examples for such offences are petty theft or traffic infractions." *See Kádár, A., Körner, J., Moldova, Z. and Tóth, B. (2008), p. 23.*

There are also questions concerning the reasons why certain individuals are stopped. A UK study reported that "[a]n alarming 27 % (2,338) of stop and search records examined [...] did not contain reasonable grounds to search people, even though many of these records had been endorsed by supervisors".[23] This, the research found, suggests that "police forces may not be fully complying with the requirements of the public sector equality duty, which requires them to have due regard to the need to eliminate unlawful discrimination and promote equality of opportunity, foster good relations and to that end, ensure that they are adequately collecting, analysing and publishing data to demonstrate that they have sufficient information to understand the effect of their work."

---

23   United Kingdom, Her Majesty's Inspectorate of Constabulary (HMIC), (2013), p. 6.

2

Lawful profiling: principle and practice

This chapter focuses on profiling by frontline police, in particular stop and search actions, and border management officers, in particular referrals to further 'second line' border checks. It explains the main principles and practices that can help to reduce the risk of unlawful profiling. These measures can be taken at both management and operational levels. It takes into account the different legal and practical contexts of stop and search actions and border checks.

In the context of border management, the Schengen Borders Code (Regulation (EU) No 2016/399)[24] establishes unified rules governing border controls at the external borders of the EU. This means that some of the principles outlined in this chapter – for example, concerning the information that must be given to third-country nationals subject to a second line check – are prescribed in law and binding on Member States. In addition, Frontex has an important role in promoting a consistently high standard of border controls. In particular, the 2016 European Border and Coast Guard Regulation requires Member States to follow the common core curricula developed by Frontex when training border guards. Published in 2012, the Common Core Curriculum contains a fundamental rights component which also includes profiling (see Section 2.2.3 on targeted training).

---

24 Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code), OJ L 77, 23 March 2016.

Focus on the grounds for a second line check at the border

The systematic nature of border controls means that every traveller undergoes a basic first line check where travel documents and any other entry requirements are checked. In addition, some travellers may be referred to a further, second line check. This can be for a variety of reasons: a hit in a database, a suspicious travel document, matching a risk profile, or exhibiting suspicious behaviour.

During the first line check, the border guard can draw on information obtained by comparing data in the machine-readable travel document (which includes biometric identifiers) with data stored in national, EU and international databases such as the Schengen Information System, the Visa Information System, and Europol and Interpol databases. In practice, a referral to a second line check often occurs as a result of a hit in one of the databases.

However, a person can also be referred to a second line check for other reasons, for example, when a person matches a risk profile or the officer has other suspicions about the person. The EU Schengen Catalogue states that in addition to carrying out border checks according to the Schengen Borders Code, the goal of first-line checks should be to profile passengers and pick out suspicious persons for thorough second line checks.* Border guards therefore need to assess a combination of other indicators and criteria to establish whether a person could be attempting an irregular entry, might pose a security risk or, for example, may be a victim of human trafficking. Whether they apply a specific existing risk profile or not, in these situations border guards use profiling.

The need to ensure a smooth circulation of travellers means border guards have limited time to conduct an objective assessment of whether to subject a person to a second line check. Information from Frontex shows that officials in the EU Member States have on average just 12 seconds to decide whether they should single out an individual for a further check.** This puts them under significant pressure to make a correct decision quickly.

*   Council of the European Union (2009), Recommendation 43.
** European Border and Coast Guard Agency (FRONTEX) (2015).

The principles and practical tools in this chapter offer information to encourage discussion and action that can help officers and their wider organisations keep their profiling activities within the law. The three key principles discussed are:

- Respect individuals' dignity.

- Ensure that profiling is based on reasonable and objective grounds.

- Guarantee accountability.

Linked to each is the underlying importance of ensuring that police officers and border guards operate within the law when using profiling.

2.1. Respecting individuals' dignity

Key points

- Ensuring a **good quality encounter** does not in itself eliminate discriminatory profiling. However, it is likely to make any encounter more successful and reduce the potential negative impact of stop and search actions. In border management, professional and respectful conduct is a legal obligation.

- **Professional and respectful conduct** generally increases a person's satisfaction with the encounter.

- **Explaining the reasons for stopping** a person helps boost confidence in police and border management operations, and reduces the perception of discriminatory profiling.

- Respect and politeness **never justify unlawful border checks or police stop and search actions**.

Respecting the dignity of individuals is not only a fundamental right in itself but a core principle of police and border management operations. In frontline operations, the way police and border management officials speak to and engage with the individuals they stop, and the information they provide, is crucial.

It should always be remembered that, no matter how polite and professional officers are, singling individuals out is still an intrusive experience that must always be based on lawful grounds. Perceptions of discriminatory profiling are also linked to

the frequency and number of interactions with the police and border management authorities. This underlines the importance of ensuring that there are always objective and reasonable grounds for stopping someone.

What do the standards say?

"Border checks should be carried out in such a way as to fully respect human dignity. Border control should be carried out in a professional and respectful manner and be proportionate to the objectives pursued."

Recital 7 of the Schengen Borders Code

"All travellers have the right to be informed on the nature of the control and to a professional, friendly and courteous treatment, in accordance with applicable international, Union and national law."

Section 1.2 of the Practical Handbook for Border Guards (Schengen Handbook)

"Police personnel shall act with integrity and respect towards the public and with particular consideration for the situation of individuals belonging to especially vulnerable groups."

Recommendation 44 of the European Code of Police Ethics

Ensuring that police officers and border guards are courteous and informative in tense and difficult situations is not always easy. However, evidence shows that setting a respectful tone significantly increases the level of satisfaction with the encounter.[25] Figure 5 illustrates some elements of a respectful encounter.

Some elements of border checks are regulated by the Schengen Borders Code, such as the requirements to carry out checks in a professional and respectful manner or to give information on the purpose of and procedure for the check (Schengen Borders Code, Recital 7, Article 7 and Article 8 (5)). Use of a common language, on the other hand, is not an absolute requirement in the border management context due to the inherently varied nature of border traffic. The Schengen Borders Code does, nevertheless, require Member States to encourage border guards to learn the languages necessary for carrying out their tasks (Article 16 (1)). The Schengen Catalogue, which contains a set of recommendations and best practices for external border control, further recommends that border guards have the ability to

---

25   FRA (2014b).

Figure 5: Three elements of a respectful encounter

1 Behave professionally and respectfully, avoiding discriminatory, degrading, humiliating, or prejudiced behaviour.

2 Where possible, use language understood by the person to ensure effective communication.

3 Explain the purpose of the search or check, and the grounds for conducting it.

RESPECT & DIGNITY

Source: FRA, 2018

communicate in foreign languages related to their daily duties. As a best practice, it refers to a satisfactory knowledge of neighbouring countries' languages, as well as other languages depending on the nature of the border traffic. Ideally, officers with appropriate language skills should be included in every shift.[26]

The lack of consideration and respect during police stops may have direct effects on the effectiveness of policing (see Section 1.3.2). The Police and Criminal Evidence Act Code of Practice developed in the United Kingdom states that: "All stops and searches must be carried out with courtesy, consideration and respect for the person concerned. This has a significant impact on public confidence in the police. Every reasonable effort must be made to minimise the embarrassment that a person being searched may experience."[27]

Some important components of respecting dignity, such as providing explanations for the stop and ensuring that individuals are given the opportunity to express their views, are basic parts of police and border management procedures. Stop and search forms can help to provide a structured way to provide this information (see Section 2.3.1).

In the border management context, standard forms are a useful tool to inform travellers of the purpose of and procedure for the second line check. They can facilitate communication with travellers, provided they are distributed with and supplemented by further oral explanations when necessary. The Schengen Borders Code

---

26   Council of the European Union (2009), Recommendations 27 and 41.

27   United Kingdom, Home Office (2014a), Section 3.1.

requires that people subject to a second line check should be given written information in a language that they understand, or could reasonably be presumed to understand, on the purpose of and procedure for the check. The information should:

· be available in all EU official languages and the languages of the countries bordering the country concerned;

· indicate that the traveller can request the name or service identification number of the official carrying out the check, the name of the border crossing point, and the date that the border was crossed.

Those elements of a respectful encounter associated with communication and interpersonal skills are more difficult to set out in operating procedures, and may require further investment in training. Difficulties in setting a positive tone for the encounter may arise from:

· limited communication skills;

· inability to articulate the reason for the action; and

· failure to overcome personal and institutional biases and negative stereotypes, as well as built-up hostilities within sections of the community.

2.2.   Reasonable and objective grounds

Key points

- Law enforcement and border management actions based on specific and up-to-date intelligence are more likely to be objective.

- To be lawful, stop and search actions and referrals to second line border checks must be based on **reasonable and objective grounds for suspicion**. 'Gut feeling' is not a reasonable or objective ground for stopping and searching a person or referring a person to a second line border check.

- Protected characteristics such as race, ethnic origin, gender or religion can be among the factors that law enforcement authorities and border guards take into account for exercising their powers, but **they cannot be the sole or main reason to single out an individual**.

- Profiling that is based solely or mainly on one or more of the protected grounds amounts to direct discrimination and is unlawful.

Objectivity is an important principle of police and border management work. In the context of profiling, individuals should only be stopped and searched or made subject to second line border checks on the basis of reasonable and objective grounds for suspicion. Objective justifications may include the individual's behaviour, specific intelligence, or circumstances that link a person or persons to suspected unlawful activity.

Ensuring objectivity in profiling requires:

- avoiding bias, including through clear guidance and targeted training; and

- making effective use of intelligence and information.

2.2.1.   Avoiding bias

The European Code of Police Ethics provides guidance on police conduct in areas including police action and intervention, police accountability and police supervision.[28] It underlines the general principle that: "[t]he police shall carry out their

---

28   Council of Europe, Committee of Ministers (2001), Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics, 19 September 2001.

tasks in a fair manner, guided, in particular, by the principles of impartiality and non-discrimination".[29]

Singling out individuals by using *as the single or determinative factor* their actual or perceived race, ethnic origin, gender, sexual orientation, religion, disability, or other prohibited grounds violates fundamental rights. It can also have significant negative consequences for both public authorities and communities (see Section 1.3).

Discriminatory profiling can reflect both individual and institutional biases. In addition to personal biases, stereotypes and discriminatory behaviour towards individuals might arise from specific practices within law enforcement and border management authorities. Making institutional procedures and practices more transparent can help address discrimination and the perpetuation of stereotypes.

Recognising deeply held biases can be difficult. Police officers and border management officials may believe that they single out individuals based on reasonable and objective grounds, (such as behaviour) when these decisions actually reflect their biases.

When stopping individuals, officers often link the reason for singling out one specific person to a 'gut feeling' or 'intuition'. This is likely to be based on a combination of expertise and past experiences but may also reflect a conscious or subconscious bias of the officer. To avoid unlawful profiling, officers should reflect on whether their decision is justified by objective information. 'Gut feeling' itself is not a reasonable or objective ground for stopping and searching a person or subjecting a person to a further check at the border.

2.2.2. Clear guidance to officers

Practical, understandable and ready to use guidance is of particular importance in helping frontline law enforcement and border management officers avoid unlawful profiling. Guidance can come in many forms: it can be attached to legislation, issued by law enforcement and border management authorities themselves, or delivered on a daily basis by senior officers. Using real-life examples to show what to do in particular situations is likely to be more effective than an explanation of rules and procedures.

---

29   *Ibid.,* para. 40.

Officers in management positions must inform staff that actual or perceived race, ethnic origin, gender, sexual orientation, religion, or other prohibited grounds for discrimination cannot be the determining factor for initiating law enforcement or border management action against an individual. Clarifying when and how personal characteristics can be used can help to reduce the risk of differing interpretations, as well as reliance on stereotypes and prejudices. Guidance should also cover issues related to privacy and data protection.

Table 3 shows some of the types of guidance that can be used and important features that should be taken into account.

Table 3:   Types, characteristics of guidance and stakeholder involvement

Types of guidance	Characteristics of guidance	Stakeholder involvement
• standard operating procedures • codes of conduct • regular guidance from senior officers	• detailed and specific • covering all activities where bias-based profiling may occur: • stop and search • arrests • border checks • use of force, etc.	• develop guidance with other stakeholders • make guidance available to communities • encourage feedback from communities on the guidance

Source: FRA, 2018

Case study

Code of practice and the ambassadors approach (Dutch police)

The Dutch police has developed a code of practice together with civil society organisations, such as Amnesty International, which describes the four principles of a professional stop:

☑ A legitimate and justifiable selection of persons.

☑ Explanation of the reason behind the stop and search.

☑ Use of professional communication.

☑ Officers to reflect on their practices and provide feedback to each other.

Altering practices that are not perceived as problematic, for instance the practice of proactive policing that may result in ethnic profiling, is difficult. Police in Amsterdam have developed a bottom-up approach involving field officers (ambassadors) in the teams, assisted by their managers and trainers. The first step is to raise awareness by showing and discussing the impact of proactive stops on the individuals targeted, and by introducing an alternative framework which is fair and effective. The second step is for officers to embrace this new practice.

For more information in Dutch, see the police's website.

2.2.3. Targeted training

Training for police officers and border guards is another important tool in minimising the risk of unlawful profiling. There are many different types of training, which can occur at different stages of an officer's career, including: initial recruit training, in-service training and on-going professional development. Irrespective of the type, training modules should take into consideration the organisational culture and offer courses that incorporate strategies to replace and counter stereotypes. Lastly, evaluation of the impact of training is crucial to monitor how training contributed to changing officers' perception and improving their practice, and to identify gaps where further training may be required. Figure 6 highlights some issues to consider when developing targeted training.
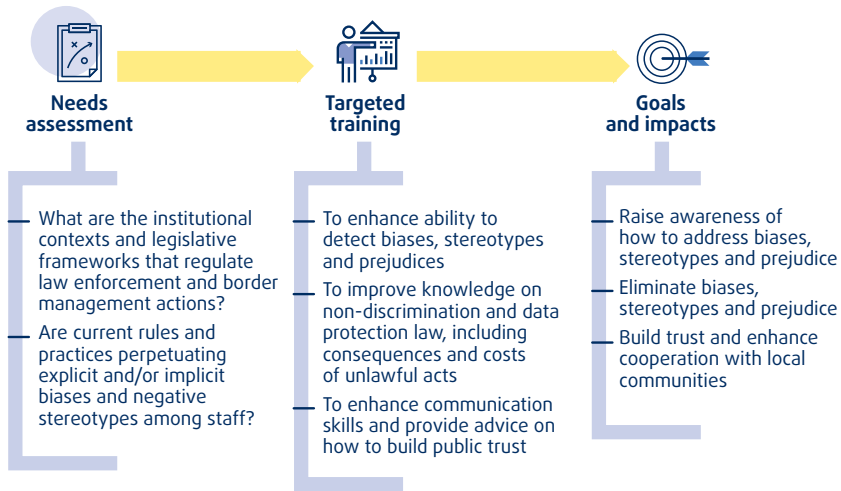
Certain types of law enforcement or border guard training are already well developed in some countries, such as 'diversity training' and 'sensitivity training'. Diversity training tries to address personal feelings about ethnicity, differences, and stereotypes, and how these influence our daily lives. However, some diversity courses do not necessarily discuss discrimination. Some studies argue that cultural and diversity training can in fact single out and reinforce differences, increasing, rather than reducing, stereotyping.[30] 'Cultural sensitivity training' (as opposed to 'general diversity training') aims to educate police and law enforcement officers about the culture of specific ethnic groups that they frequently encounter but with whom they are not familiar. Such training addresses the 'dos and don'ts' and provides guidance on politeness as viewed through different ethnic, religious, or national perspectives. Cultural sensitivity training is most effective when developed and delivered with the assistance and participation of people from the relevant communities.

---

30   Wrench, J. (2007).

Figure 6: The process and objectives of developing targeted training

Needs assessment

— What are the institutional contexts and legislative frameworks that regulate law enforcement and border management actions?

— Are current rules and practices perpetuating explicit and/or implicit biases and negative stereotypes among staff?

Targeted training

— To enhance ability to detect biases, stereotypes and prejudices

— To improve knowledge on non-discrimination and data protection law, including consequences and costs of unlawful acts

— To enhance communication skills and provide advice on how to build public trust

Goals and impacts

— Raise awareness of how to address biases, stereotypes and prejudice

— Eliminate biases, stereotypes and prejudice

— Build trust and enhance cooperation with local communities

Source: FRA, 2018

Case study

Training on lawful profiling

Training on profiling for police officers (Italy)

Since 2014, the Italian Observatory for Security against Acts of Discrimination (*Osservatorio per la sicurezza contro gli atti discriminatori*) has been implementing a training module on ethnic profiling for police officers and cadets. It focuses in particular on assumed biases that may influence profiling; the consequences in terms of efficiency of police activities; and the negative impact on relationships with communities. About 5,000 people have participated in the training module so far. Since 2017, an e-training module has also been provided in the framework of refresher courses for police.

For more information, see the website of the Italian National Police.

Fundamental rights tool in border guard training (EU)

The Common Core Curriculum (CCC) for European border guards sets out the minimum standard of skills and knowledge that every European border guard must have. It contains chapters on Sociology and on Fundamental Rights. There are specific sections on non-discrimination (1.5.4) and on ethnic profiling (1.7.10), which trainers can use. The CCC highlights potential risks linked to prejudices, racism, racial discrimination, xenophobia, Islamophobia, homophobia, and other related intolerances when conducting profiling. The 2017 update of the CCC includes sections on new competencies, especially in the field of fundamental rights.

In addition, Frontex developed a trainers' manual in consultation with universities and international organisations (see Frontex, 2013). It provides trainers with methodologies to improve the knowledge and skills of border guards in the field of fundamental rights and international protection. The manual explicitly mentions profiling and sets out basic rules for avoiding discrimination. Training is provided on a regular basis. However, there is no permanent mechanism in place to assess the attainment of training goals.

For more information, see Frontex (2012).

Profiling study days for senior officers (Belgium)

In 2015, the Centre for Policing and Security (CPS) based in Ghent (Belgium), with the involvement of the Belgian equality body (Unia), organised a study day on ethnic profiling (*Profilage ethnique: l'égalité sous pression?*). It covered different aspects of the issue, including: whether and how police officers with migrant backgroundscan improve relationships with ethnic minority communities; how often ethnic profiling is used by police officers, and how it has been evaluated.

In 2016, Unia organised two study days for senior police officers from northern Brussels to raise awareness on ethnic profiling and promote reflection on the identification of profiling practices by frontline officers. Police officers from Spain and the United Kingdom introduced good practice examples to an audience composed of law enforcement officers, researchers and NGOs. In particular, they demonstrated that by reducing profiling based on ethnic origin, successful arrests of wanted persons increased. They

pointed out that this was made possible by keeping correct records of every stop, as well as ensuring transparency concerning the motives behind the stops. The training aimed at establishing a common understanding of ethnic profiling practices to support the future development of research on the practices currently implemented by the police in this area

For more information, see Belgium (2015 and 2017).

Training should address biases and stereotypes that might be embedded in law enforcement and border management institutions themselves. The broader institutional context and the internal policies in place – such as existing complaints mechanisms, the presence of a "code of silence" among colleagues, etc. – should be examined before conducting training on preventing unlawful profiling. Curricula should address biases and stereotypes integrated in policing actions such as stop and search actions, arrests, detention and the use of force.

High-ranking or mid-level officers have a key role to play in making training successful, as both participants and in the importance they attach to training.[31] As recipients, senior officers can learn new practices and skills which they can pass down to frontline officers. Organisational culture, largely set by senior management, has a substantial impact on the everyday behaviour of police officers and border guards, including how they interact with the public.

Senior officers can also ensure that training is viewed positively. The behaviour of staff in management positions, for example how supervisors communicate the purpose of training to officers or whether officers think they are selected randomly or because they are 'problematic officers' can affect the level of interest and engagement in the training. Encouraging officers to participate actively in training programmes and be open to behavioural change to improve their daily work is likely to enhance the impact of training.[32]

Once training is completed, it should be reviewed and evaluated to assess its impact on raising awareness and changing behaviour.

---

31   See European Commission (2017b).

32   Miller, J. and Alexandrou, B. (2016).

Focus on the guiding principles of training

Specialised training is key to ensuring a lawful use of profiling. The European Commission developed a compilation of key guiding principles on how to ensure effective and quality training as regards hate crime. The same principles apply to training on lawful profiling.

Hate Crime Training for Law Enforcement and Criminal Justice Authorities: 10 Key Guiding Principles

Ensuring Impact and Sustainability:

☑ Embed training within a broader approach to tackling discrimination.

☑ Develop a methodology to address training needs.

Identifying targets and building synergies:

☑ Customise programmes based on your personnel.

☑ Cooperate with civil society in a structured manner.

Choosing the right methodology:

☑ Combine different methodologies.

☑ Train the trainers.

Conveying quality content:

☑ Design a training curriculum of quality content.

☑ Develop training modules targeting discrimination.

Monitoring and evaluating outcomes:

☑ Link training to performance review processes.

☑ Ensure regular monitoring and evaluation of your training methods.

For more information, see European Commission (2017a).

Training in isolation will not, however, be effective in countering officers' implicit biases. What is needed is a shift in institutional thinking. Authorities must therefore consider multifaceted interventions to counter personal and institutional biases (see case study).

Case study

Addressing 'institutional racism' in the police

Following concerns about the role of race in police mishandling of the investigation into the racist murder of Stephen Lawrence in the United Kingdom, the UK government set up a wide-ranging inquiry to identify "the lessons to be learned for the investigation and prosecution of racially motivated crimes".

The report of the inquiry, published in 1999, highlighted the issue of 'institutional racism' in the Metropolitan Police, including the disparity in stop and search figures, as a matter of considerable concern to affected communities. The recommendations of the inquiry, ranging from racism awareness training to reporting and recording of incidents, were framed by an overall call for increased openness, accountability and the restoration of confidence by the police service.

Reviews published in 2009, ten years after the inquiry, highlighted improvements in the way police interact with ethnic minority communities and investigate racially motivated crimes. However, they note that Black people remain much more likely to be stopped and searched than their White counterparts.

For more information, see United Kingdom, Home Office (1999), United Kingdom, Equality and Human Rights Commission (2009), and United Kingdom, House of Commons Home Affairs Committee (2009).

2.2.4. Reasonable grounds for suspicion: making use of intelligence and information

When police officers and border management officials single out an individual, they typically base their decision on a combination of elements. This can include more 'objective' information such as specific intelligence, behaviour, clothing or the objects that the individuals carry with them, as well as 'subjective' knowledge based on experience.

All of these elements can represent a 'signal' of illegal activity. However the information must be combined and used with caution. Evidence shows that officers can find it difficult to distinguish between objective and subjective elements in practice, as in the Example quoted in the box.

Examples

"It's very subjective. It's your feelings about a person and a case, but there are also evidential issues of discrepancies in what they're saying, inconsistencies between them and what their sponsor says, inconsistencies between what they're saying and their paperwork, between what they're saying and all the stuff they might have in their bags. So there's evidence, but [these things alone would not] completely go against someone. It's the whole picture that the officer has to build about a person."
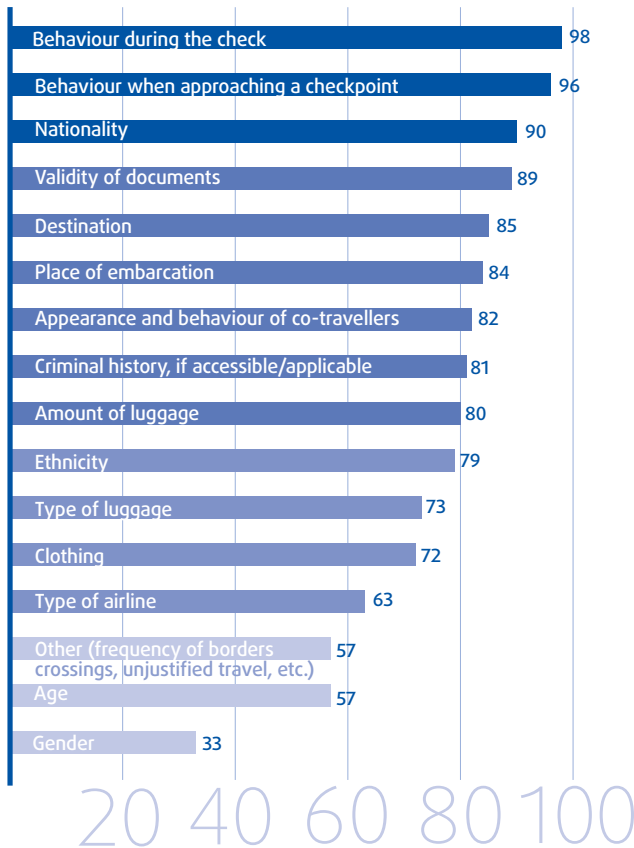(Immigration officer at major UK airport)

For more information, see FRA (2014a), p. 46.

Focus on identifying persons attempting to enter a country in an irregular manner

FRA research conducted in 2012 at major airports reveals that border guards take into account a number of factors when deciding whether an individual could be attempting to enter the country in an irregular manner. These often include a combination of 'objective' criteria – such as the person's behaviour when approaching the checkpoint and during the check, type and amount of luggage, and the validity of travel documents – and personal experience of past border checks, as Figure 7 shows.

Figure 7: Indicators considered helpful or very helpful for effectively recognising persons attempting to enter the country in an irregular manner before officers speak to them (%)

Indicator	%
Behaviour during the check	98
Behaviour when approaching a checkpoint	96
Nationality	90
Validity of documents	89
Destination	85
Place of embarcation	84
Appearance and behaviour of co-travellers	82
Criminal history, if accessible/applicable	81
Amount of luggage	80
Ethnicity	79
Type of luggage	73
Clothing	72
Type of airline	63
Other (frequency of borders crossings, unjustified travel, etc.)	57
Age	57
Gender	33

Note: *Valid responses range between 206 and 216 out of 223. Respondents who did not provide an answer to a given item have been excluded when computing the results. Non-responses range from seven to 17 persons, depending on the item.*

Source: *FRA, Border guard survey, 2012 (question 17)*

Border guards identified behaviour during the check or when approaching a checkpoint as the most helpful factor in recognising people trying to enter the country in an irregular manner. However, factors such as nationality and ethnicity, which could indicate discriminatory profiling, were also viewed as significant.

Clothing, which was also considered a useful indicator, is an example of how apparently 'objective' information may be used in a biased way in practice. Certain types of clothing may be linked to specific risk profiles. For example, victims of trafficking in human beings of a certain nationality may typically wear particular types of clothing. However, clothing can also indicate that a person belongs to a specific ethnic or religious group. Even if there are sufficient other reasons to justify a referral to a second line check, persons who strongly identify with their ethnic or religious background, have prior negative experience or do not receive an adequate explanation from the officer, may perceive the treatment as discriminatory.

For more information, see FRA (2014a). In relation to profiles of trafficking victims, see Frontex (2017).

Good intelligence on patterns of behaviour or events can increase objectivity in profiling. This could relate to criminal activities or, in the case of border management, to irregular migration or cross-border crime. When law enforcement and border management actions are based on specific and timely intelligence, such as information about a specific person and/context, they are more likely to be objective and less likely to be based on stereotypes.

In addition to intelligence and objective elements, information about protected characteristics such as actual or perceived race, ethnic origin, nationality, gender or religion may be used legitimately as an added component in profiling assessments in certain circumstances. For use of this information to be lawful, it must be regulated by law, respect the essence of the rights and freedoms affected, be proportionate (i.e. complying with a balance of interests) and necessary (i.e. there should not be any less restrictive means available). There must be a justifiable reason, other than the protected grounds, for the officers to treat an individual differently from other members of the public. The reason must also specifically relate to the particular individual, as in the example outlined in the box.

Examples

Witnesses report that the suspect in a robbery was wearing red running shoes and a black baseball cap, is 1.60 to 1.70 meters tall, and perceived to be of Chinese origin. Under these circumstances, law enforcement authorities could legitimately consider ethnic background as relevant to determining whether an individual becomes a potential suspect, as it is combined with specific intelligence.

Focus on detailed suspect descriptions

Good suspect descriptions can reduce the risk of unlawful profiling. A suspect description consists of details about the person, such as the colour of skin, hair and eyes, height and weight, and clothing. These details are provided by the crime victim or witnesses, or on the basis of other specific intelligence. A good suspect description can be used by officers as the basis for stop and search actions aimed at detaining suspects, or for referring persons at border controls for a second line check.

However, when law enforcement officers receive an overly general suspect description that features race, ethnicity, or similar characteristics, they should not use that description as the basis for operations. In such cases, operations are likely to result in many stops of innocent people who happen to share the same characteristics. Rather, they should seek further specific operational intelligence to guide the investigations.

For more information, see European Commission (2017b).

Information that seems objective can actually incorporate biases. Apparently objective factors, such as time, day, location, etc. can be used as a proxy for prohibited grounds of discrimination such as actual or perceived race, national origin, gender, sexual orientation or religion, as the example below shows.

Examples

A stop and search operation is conducted around midday on Friday in area X. However, this period is the most important prayer time for Muslims. As area X is close to a mosque, the supposedly objective factors of time, date and place could actually act as proxies for a stop and search operation based on the prohibited discriminatory ground of religion.

Similarly, looking for certain suspicious behaviour may seem like an objective way to identify possible wrongdoings. However, officers may interpret a person's behaviour in different ways, depending on other characteristics of the person concerned. Evidence shows that working knowledge and understanding of intelligence may differ greatly between officers and often does not correspond to actual crime patterns.[33]

---

33   United Kingdom National Policing Improvement Agency (NPIA) (2012).

Providing timely and detailed intelligence to officers, for instance at 'pre-shift briefings' at the start of each shift, should reduce discretion and provide officers with guidance on how to target their powers more specifically at current crime patterns and identified safety issues. This reduces the role of bias. Improving the quality and use of intelligence to focus on behavioural factors or specific information is most effective when combined with increased supervision and monitoring of how officers use their powers.

Case study

Ensuring objectivity in profiling

Pre-shift briefings (EU)

The Schengen Catalogue recommends that before each shift, the officer on duty provides information on any risk indicators and risk profiles. Ensuring overlaps between shifts can provide enough time for exchanges of information between staff on outgoing and incoming shifts, and adequate briefing.

For more information, see Council of the European Union (2009).

The SDR training programme (The Netherlands)

The Search, Detect and React (SDR) training programme is aimed at preventing crime or terrorist acts before they occur by enhancing the capacity of security personnel with respect to behavioural profiling. This means drawing attention away from unalterable characteristics such as skin colour, and focusing instead on individual behaviour when making choices about police action. As indicators of suspicious behaviour are context-specific, the training is nuanced according to the environment. It rejects the idea that a one-size-fits-all solution exists. Having detected relevant patterns of conduct, officers are required to act in a 'sensitive' manner. In most cases, they will have an informal conversation with the suspect rather than use any formal police powers. The programme entails classroom teaching in addition to applied and on-the-job training.

For more information, see the SDR Academy's website.

The stop and search Authorised Professional Practice (APP) tool (United Kingdom)
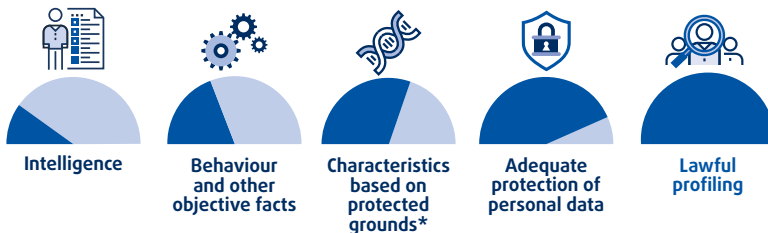
The College of Policing in the United Kingdom has developed Authorised Professional Practice (APP) guidance covering various aspects of police work. The APP on stop and search explains what a stop and search is, why it is important to use these powers correctly, and the features of lawful stops and searches. It explains that the lawfulness and effectiveness of stop and search encounters will be supported by ensuring:

- **Fairness**: the officer's decision to stop and search a person must be based only on appropriate, objective factors. A person can never be stopped solely or mainly on the basis of protected characteristics or factors such as previous convictions.

- **Legality**: the stop and search must have a legal basis that is applied lawfully.

- **Professionalism**: during stop and/or search encounters, officers must comply with professional standards of conduct, especially the Code of Ethics, communicate effectively with people and treat people with dignity and respect.

- **Transparency**: the individual encounter must be accurately recorded. Effective supervision and monitoring of stops and searches, as well as public scrutiny, must be ensured.

For more information, see United Kingdom, College of Policing (2016).

Figure 8 illustrates the different elements that can be used in lawful profiling; how they are combined will depend on the nature of the specific case.

Figure 8:   Combination of elements

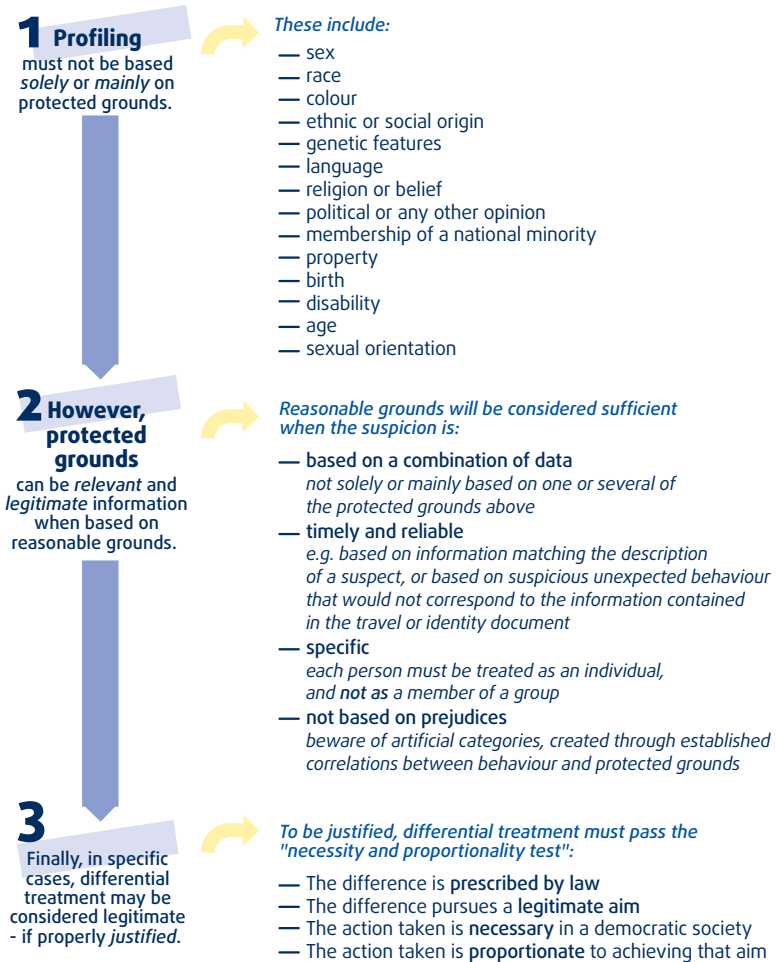| Intelligence | Behaviour and other objective facts | Characteristics based on protected grounds* | Adequate protection of personal data | Lawful profiling |

*   See Figure 9 for the list of protected grounds under EU law. Profiling should <u>never</u> be based solely or mostly on protected characteristics.

Source: FRA, 2018

Figure 9 shows how these elements can be combined to ensure that profiling is not discriminatory.

Figure 9: Elements of non-discriminatory profiling

1 Profiling must not be based *solely* or *mainly* on protected grounds.

These include:
— sex
— race
— colour
— ethnic or social origin
— genetic features
— language
— religion or belief
— political or any other opinion
— membership of a national minority
— property
— birth
— disability
— age
— sexual orientation

2 However, protected grounds can be *relevant* and *legitimate* information when based on reasonable grounds.

Reasonable grounds will be considered sufficient when the suspicion is:

— **based on a combination of data**
  not solely or mainly based on one or several of the protected grounds above
— **timely and reliable**
  e.g. based on information matching the description of a suspect, or based on suspicious unexpected behaviour that would not correspond to the information contained in the travel or identity document
— **specific**
  *each person must be treated as an individual, and **not as** a member of a group*
— **not based on prejudices**
  beware of artificial categories, created through established correlations between behaviour and protected grounds

3 Finally, in specific cases, differential treatment may be considered legitimate - if properly *justified*.

To be justified, differential treatment must pass the "necessity and proportionality test":

— The difference is **prescribed by law**
— The difference pursues a **legitimate aim**
— The action taken is **necessary** in a democratic society
— The action taken is **proportionate** to achieving that aim

Notes: *The list of protected grounds varies across Member States. For an overview of the grounds of discrimination that are included in the criminal codes of each and every Member State, see FRA (2018d). See also the website of Equinet, the European Network of Equality Bodies, which lists the grounds of discrimination covered by national equality bodies.*

Source: *FRA, 2018*

2.2.5. Stop and search forms for law enforcement profiling

Stop and search forms can help officers to reflect on whether the stops they are conducting are based on reasonable grounds, and allows senior officers to monitor potential discriminatory practices in individual officers' use of stop and search. While sometimes considered burdensome, they also provide a record of stops which, when collated, provides data that can point to whether stops are being conducted in a lawful way.[34] This can help to promote openness and accountability. In addition to the completion of paper forms, new technologies such as mobile apps can be used to record this information.

Some important points to incorporate when designing stop and search forms are described in the focus box.

Focus on what makes a good stop and search form

Stop and search forms need to be well designed to be useful. Firstly, completing the forms creates additional workload for officers. If not clearly designed and reasonably short, the risk is that officers may not complete the entire form, or will fill it out in a cursory way. Secondly, good forms allow data to be easily extracted and collated to support the monitoring and evaluation of stop and search actions.

Whenever possible, stop and search forms should:

- Use multiple-choice fields which are quicker to fill in and easier to process statistically.

- Set out an exhaustive list of options for each item.

- Avoid ambiguous items.

- Be easily understandable, for both the officer and the person stopped.

- Include:

  o the legal grounds for the search. Simple explanations rather than a list of rules are preferable;

  o the date, time and place where the person or vehicle was searched;

---

34   United Kingdom, Stop Watch (2011).

o the object of the search e.g. item(s) officers are looking for;

o the outcome of the stop;

o the name and police station of the officer(s) conducting the search;

o the personal details of the individual(s) searched, such as name, address, and nationality, may be recorded. However, the individual can refuse to provide this information.

To be effective, forms should be completed at the time the stop is conducted.

A copy should be given to the person stopped or the person in charge of the vehicle searched. In the United Kingdom, individuals who have been stopped are entitled to request a copy of the record within three months of the stop. In this way, the form does not only support evidence of the stop for the police, by also for the individuals stopped.

For more information, see United Kingdom, West Midlands Police (2012), p.7; and United Kingdom, Home Office (2014a).

Case study

Stop and search form (UK)

The stop and search form used by West Midlands Police in the United Kingdom is replicated below.

It shows that the person stopped is asked to self-identify as belonging to one of the listed categories of ethnicity, including options of 'other' or 'not stated'. The officer conducting the stop can add their perception if they disagree with the self-identification.

The Code of practice for the exercise of stop and search powers in the UK states that officers should explain to those stopped that information on ethnicity "is required to obtain a true picture of stop and search activity and to help improve ethnic monitoring, tackle discriminatory practice, and promote effective use of the powers".

WC332
03/17

Stop and Search
Call: 805 6666

Power
1 Drugs
2 Section 1 PACE

A typical response would be "2,5" if the Power was 'S1 PACE' and Object 'Fireworks'. The Object of search will default if there is only 1 option.

3 S47 Firearms Act
4 Section 60 CJPO Act 1994
5 Section 43 Terrorism Act
6 New Psychoactive Substances Act 2016
7 Other (eSearch contains list of additional powers)

Object
1 Search for Drugs
1 Stolen Items
2 Offensive Weapon/Bladed Article
3 Articles for Burglary/Theft/Fraud/TWOC
4 Items for Criminal Damage
5 Fireworks
1 Firearms
1 Dangerous Items/Offensive Weapons
1 Evidence of Terrorism
1 Search for NPS

Self Assessed Ethnicity (16+1)
A1 Asian - Indian
A2 Asian - Pakistani
A3 Asian - Bangladeshi
A9 Asian - Any Other Asian background
B1 Black - Carribean
B2 Black - African
B9 Black - Any Other Black background
M1 Mixed - White & Black Caribbean
M2 Mixed - White and Black African
M3 Mixed - White & Asian
M9 Mixed - Any Other Mixed Background
O1 Other - Chinese
O9 Other - Any Other Ethnic Group
W1 White - British
W2 White Irish
W9 White - Any Other White background
NS Not Stated

Officer assessed Ethnicity (PNC)
IC1 White North European
IC2 White South European
IC3 Black
IC4 Asian
IC5 Chinese/Japanese/South East Asian
IC6 Middle Eastern
IC9 Other

Grounds for Search - Multi Select
1 Acting Suspiciously
2 Stopped in tasking area
3 Stopped in high crime area
4 Could not give reasonable explanation
5 Tried to avoid police
6 Seen to discard an item
7 Seen to conceal item
8 Smell of controlled drug
9 Current Intelligence
10 Matches Description

Grounds will be supported by a free text explanation

Outcome
1 Arrested - Consequence of Stop & Search
2 Arrested - Unrelated Offence including Warrant/PNC
3 Community Resolution
4 Fixed Penalty
5 Cannabis Warning
6 Street Bail
7 Street Summons
8 Conditional Bail
9 Out of custody Caution
10 Substance seized, person not arrested
11 NFA

For more information, see United Kingdom, West Midlands Police (2017a); and United Kingdom, Home Office (2014a), p. 19.

Many forces are now moving away from collecting stop and search data on forms, and instead use technologies such as mobile phone apps, radio-based systems, mobile data terminals or laptops. These technologies can speed up the recording process and reduce bureaucracy, but also create new risks, notably in relation to the algorithmic use of personal data (see Chapter 3).

Case study

Live recording of stop and search actions

"eSearch" (West Midlands Police, United Kingdom)

Adopted in April 2014, this system is based on a call between the officer on the ground and a member of staff in the Contact Centre (control room). The details of the stop and search are recorded immediately in the Contact Centre and included in a database. This information can then be accessed and used to scrutinise the effectiveness of stop and search actions, both internally and externally. eSearch has transformed the recording of stop and search actions. Records can be viewed far more quickly on police systems, with benefits for intelligence and integration into operational policing.

For more information, see United Kingdom, West Midlands Police (2014) and United Kingdom West Midlands Police (2016).

Mobile app for frontline officers (West Midlands Police, United Kingdom)

A new mobile app launched in October 2017 aims to make stop and search quicker and more efficient. The eSearch app allows officers to record details of street encounters directly into the app via their smart phones, without the need to call contact centre staff. Each stop is given a unique reference number, and GPS automatically records its location. The app is expected to reduce calls to the contact centre by almost 1 000 calls a month.

For more information, see United Kingdom, West Midlands Police (2017b).

Senior officers play an important role in ensuring that stop and search operations are lawful. The example below shows how senior officers can maintain oversight. They should also ensure that stop and search actions is not used as a performance measure based on the number of stops conducted.

Case study

Signing off stop and search records (UK)

Since August 2014, every stop and search record in the United Kingdom must be signed off by the supervisor of the officer who conducted the search. Records are endorsed as either meeting or not meeting the relevant standards. In the latter case, the reporting officer must record why on the stop and search record.

For more information, see United Kingdom, Home Office (2014a).

2.3. Accountability

Key points

- Law enforcement and border management officials are **accountable** for keeping profiling within the law.
- **Collecting reliable, accurate and timely data** on profiling activities is crucial for ensuring accountability.
- **Effective complaint mechanisms** can both deter abuses of power and secure and restore public trust in the operations of police and border management authorities.
- **Feedback meetings with members of the public** to listen to their opinions, discuss profiling, and gather feedback on operations, provide opportunities to learn important lessons and improve profiling actions.

Accountability is a key principle of democratic governance. In very general terms, it involves the provision of answers to those who are entitled to demand an account.[35] Accountability focuses not only on individual decision-making, but on that of the institution (so-called 'institutional accountability'). As public officials and bodies, law enforcement and border management officers, as well as their organisations, are accountable to the public for their decisions and actions. This includes being accountable for ensuring that profiling is within the law.

---

35   Bovens, M., Schillermans, T. and Goodlin, R.E. (2014), pp. 1–11.

Collecting reliable, accurate and timely data is crucial for ensuring accountability. As much of the data contain sensitive personal information, they must be handled in accordance with data protection rules and procedures (see Chapter 3).

Accountability Checklist

The checklist below provides a basic overview of steps that law enforcement and border management authorities may take to ensure that they are accountable for decisions and actions concerning profiling. This list can guide officers towards improving their accountability, but should not be understood as mandatory steps for both law enforcement and border management officers. Depending on the context, some recommendations may not apply to the specificities of border management.

1. Identify

☑ Recognise and **acknowledge** the problem of unlawful profiling. Bias and stereotypes do exist and pose risks for those involved, including officers and local communities.

☑ **Collect and make use of disaggregated data**: it is an important tool to assess effectiveness and performance.

☑ Participate in external panels organised by the community or civil society to get **feedback** on your practices and enhance trust in your operations.

2. Collect information

☑ Guarantee accountability by **keeping records** of profiling activities.

☑ Subject to the necessary safeguards, **video surveillance** and/or **body worn cameras** can enhance accountability, and provide evidence to support action to modify patterns of biased behaviour.

☑ Create **stop and search forms** to be completed by police officers after every stop.

3. Act and Prevent

☑ Conduct **assessments** to find out if there are any rules and practices that perpetuate explicit or implicit bias and negative stereotypes.

☑ Introduce specific courses and/or **training sessions** focusing on addressing personal and institutional bias and stereotypes.

☑ **Provide information** to individuals who are stopped to increase the perception of a fair stop, and give individuals sufficient information to decide whether or not to seek remedy. For referrals to second line checks at border crossing points, the provision of information is a legal obligation.

☑ Show **zero tolerance** within the organisation for bias-based incidents.

☑ Establish **internal mechanisms** for supervision and control, such as internal panels for discussing whether stops are made on the basis of reasonable grounds.

☑ Make sure that **performance indicators** are linked to avoiding bias and stereotypes.

☑ Establish **complaints mechanisms** to deter abuses of power and ensure accountability.

Source: FRA, 2018

2.3.1. Internal monitoring

The leadership and management of police and border management authorities play an important role in establishing an ethos that upholds individual rights and the principle of non-discrimination, both within the organisation and in its dealings with the public. They also contribute to establishing a climate of accountability and transparency. Open communication between staff (both horizontal and vertical) and setting clear standards for behaviour, such as professional codes of conduct, are two of the internal elements that should be in place to enhance accountability. Recruitment and training also play important roles (see Section 2.2.3).

Under EU law any public authority or body has to designate a **Data Protection Officer.** He or she advises police and border management forces on their data protection obligations, including keeping records of data-processing activities or carrying out data protection impact assessments. In the context of profiling, the Data

Protection Officer will, for example, advise on and oversee that personal data collected for, or during, profiling are lawfully processed and stored.

Focus on the role of Data Protection Officers

The **Police Directive** requires Member States to appoint a data protection officer whose tasks include:

- monitoring compliance with applicable legislation concerning the protection of personal data, including:
  - assigning responsibilities;
  - awareness-raising and training of staff;
  - audits;
- providing advice on the data protection impact assessment and monitoring its implementation;
- acting as a contact point for the supervisory authority.

The data protection officer should be involved fully and in a timely manner in all issues related to the protection of personal data.

See Articles 32-34 of the Police Directive.

Within police forces, internal monitoring of profiling can be carried out as part of a wide range of other measures aimed at keeping records of encounters between authorities and the general population (see Figure 10). These include the use of:

- **stop and search forms**: that are a useful practical tool for encouraging officers to carry out well-grounded stops, and promoting openness and accountability with the public (see Section 2.2.5);

- **body-worn cameras**: subject to the necessary safeguards, they can enhance trust between communities and the police, and may act as a deterrent for the misuse of force and discrimination (see Section 2.3.2).

Figure 10: Elements of internal monitoring

INTERNAL
MONITORING

Appropriate human rights knowledge for officers in charge of monitoring

Body-worn cameras

Stop and search forms

Data Protection Officer

Effective complaint mechanisms

Monitoring standards should be clearly established and made available to officers

Timely, clear and open post-profiling discussion between staff and supervisors

● Specific to Law Enforcement

● Apply to both Law Enforcement and Border Management

Source: FRA, 2018

Internal monitoring activities in border management organisations can also make use of these measures. For example, the Schengen Catalogue recommends recording the number of and reasons for referral to second line checks. In addition, the different contexts of border controls, the infrastructure at border crossing points and the on-site presence of superiors create other opportunities for internal monitoring. For instance, additional technological equipment such as video surveillance may be available.

With the necessary safeguards in place, video footage may provide evidence for assessing how profiling is conducted, and provide evidence in the case of specific complaints. For example, it could confirm whether a person's behaviour while waiting for the first line check gave sufficient reason for referring them to a second line check.

Unlike in stop and search actions, the presence of video surveillance is largely expected by passengers at border crossing points due to their public nature and security considerations. Nevertheless, the use of such tools must comply with the right to privacy and applicable data protection rules.

Keeping records can have both short and long-term benefits. The example of stop and search forms shows how:

- In the **short-term**, stop and search forms can provide on-the-spot accountability. In the United Kingdom, everyone stopped is given a record of the stop form or a receipt identifying where they can access a copy. It provides the details of the reason for the stop as well as information on where and how to complain. This allows the person to see the reason and to challenge it if they consider it unfair.

- In the **long-term**, analysis of records allows the police force to identify whether stop and search powers disproportionately target members of minority groups, and to adjust guidance given to officers accordingly. These records can be made public to enhance transparency and promote public confidence in the use of stop and search powers.

Keeping records: What does the law say?

To ensure the lawfulness of data processing, the Police Directive requires that law enforcement authorities keep a record of all categories of processing activities under their responsibility. Moreover, in automated processing systems, they have to keep logs with a view to knowing who consulted or disclosed personal data, when it happened, who received the data, and the justification behind data processing (see Section 3.1.3).

Articles 24 and 25 of the Police Directive

Case study

Using records to detect disproportionality in stop and search actions (UK)

The Police and Criminal Evidence Act Code of Practice developed in England and Wales (United Kingdom) places a statutory duty on police forces to monitor the use of stop and search powers to detect whether they are being "exercised on the basis of stereotyped images or inappropriate generalisations". Any apparently disproportionate use of the powers by particular officers or groups of officers or in relation to specific sections of the community should be identified and investigated, and appropriate action taken to address it. In addition, police must make arrangements for

the records to be scrutinised by representatives of the community, and to explain the use of stop and search powers at a local level.

For more information, see United Kingdom, Home Office (2014a).

Police in the United Kingdom have developed several tools to increase transparency by making stop and search data easily accessible. The website www.police.uk allows users to enter their postcode to see detailed information about the number and nature of stops in their local area. The information published draws on completed stop and search forms. In addition, the Metropolitan Police's stop and search dashboard provides data on all stop and searches in London, including on the proportion of people with ethnic minority backgrounds stopped relative to the overall population. Users can access detailed data online in different ways, such as:

- a map showing, on a monthly basis, the exact location of the stop and searches conducted in a particular area. The tool also provides detailed information on the stop and search (object, type, outcome, whether the stop and search was part of a policing operation), on the person (gender, age range, self-defined ethnicity, officer-defined ethnicity), and the legislation supporting the lawfulness of the stop and search (see Figure 11); and

- an overview of statistics and charts presenting the stop and search actions of the police. This allows the information to be aggregated and downloaded.

Although this practice fosters transparency and trust, it could impact the rights to privacy and data protection of the individuals concerned. It is possible that the identity of an individual could be inferred from the combination of data available in this or other online tools. Such risks need to be assessed and, where relevant, addressed.

2.3.2. Body-worn cameras

Police forces are increasingly using body-worn cameras. They can play a role in ensuring accountability, improving the quality of individual encounters, and modifying patterns of biased behaviour. They may also help to de-escalate dangerous situations. As well as footage collected by police, members of the public are increasingly filming stops and other interaction with the police. This can also be used to review police practice.

Figure 11: Online tool showing details of stop and search actions conducted in London

Source: United Kingdom, Home Office, webpage on stop and search map

Case study

The effectiveness of body-worn cameras

In the United Kingdom, a study conducted in 2015 on the use of 500 cameras by 814 officers from the Metropolitan Police showed "no overall impact on the number or type of stop and searches conducted; no effect on the proportion of arrests for violent crime; and no evidence that the cameras changed the way officers dealt with either victims or suspects". Reports assessing the impact of similar trials by other police forces show little or no evidence that these had any positive effect in reducing crime, complaints towards officers, or the use of force.

For more information, see Big Brother Watch (2017).

In France, body-worn cameras were deployed in 300 localities for a two-year pilot period. In June 2018, a review by the Ministry of Interior highlighted the positive impacts and results of the trial. Notably, the report emphasised the

deterrent effect of the wearing of body-worn cameras on stopped individuals from abusing or insulting the police. Reports from municipalities indicated that the use of individual cameras reduced aggressiveness and insulting behaviour towards police officers. Some municipalities pointed out that the use of body-worn cameras seemed to have de-escalated situations that could otherwise have resulted in an offense against police officers. While these reports suggest that the usefulness of body-worn cameras lies particularly in the dissuasive impact of wearing them, some footage was used as evidence in court proceedings to identify offenders. Finally, several municipalities stressed the educational usefulness of the device, as some police officers were trained on intervention procedures and techniques by viewing the recordings made during interventions. Following the pilot, a draft law has been presented to the French Parliament with the aim of harmonising the use of body-worn cameras across all police forces and to extend their use to firefighters and prison officers.

For more information, see France, Ministry of Interior (2018).

A large 12-month trial of body-worn cameras in 2012-2013 in Rialto in the United States looked at whether body-worn cameras would lead to socially-desirable behaviour among the officers wearing them. The results show that, in comparison to 2011, during the 12-month trial period the use-of-force dropped from 60 to 25 instances, and complaints against the police fell from 28 to 3.

For more information, see Farrar, T. (2018).

However, the use of body-worn cameras by police raises some important fundamental rights and operational concerns. Clear safeguards and policies concerning their use are necessary to address these issues:

- The **role of body-worn cameras in detecting and deterring unlawful profiling** is unclear. Cameras capture individual incidents and do not allow for the collection of statistical data that could be used to determine whether stop and search operations are discriminatory. Rather, they can be used to review and discuss individual encounters, helping to improve their quality.

- The use of body-worn cameras could have **negative impacts on relations with minority communities**, if they feel they are being specifically targeted. Developing safeguards and policies in consultation with local communities can help to promote body-worn cameras as a tool to improve accountability rather than a means to stigmatise minority groups.

- Using body-worn cameras has **consequences for the rights to privacy and data protection**, as well as other fundamental human rights. For example they could affect the freedom of peaceful assembly if used to monitor public demonstrations, for example. It is often unclear when cameras should be switched on and off, and what happens if an officer forgets or decides not to switch on the camera: clear guidance is needed in this area. Private companies providing this service must be clear that they cannot process the footage for their own purposes. The use of body-worn cameras should be regulated by law to ensure that it is in line with fundamental rights.

Focus on using body-worn cameras effectively

Complying with three important principles can help to ensure body-worn cameras are used effectively:

- **Authenticity**: images must be clearly tied to the incident. The date and time (e.g. through timestamping) and exact location (e.g. via GPS) of the incident should be recorded.

- **Reliability**: images should be uploaded in the central system in a rigorous, safe and confidential way. These images should comply with the principles of data protection and respect for private life, and therefore should not be kept for a longer period than specified by law.

- **Admissibility**: to be useful in criminal proceedings, footage must be admissible in courts. This can involve:

  o Avoiding continuous video recording, which constitutes unacceptable interference with the right to privacy of both police officers and the individuals filmed.

  o Informing those who may be filmed, and obtaining their consent (when necessary).

  o Storing images with an adequate level of security, and keeping track of access to images by both police officers and citizens.

For more information, see Coudert et al. (2015), p. 8.

Further technological developments will require the development of new safeguards to ensure body-worn cameras are used lawfully. For example, cameras that can automatically recognise a person's face by comparing and matching it with previous entries in an existing database pose new challenges to the rights to privacy and data protection.

Case study

Police Body-Worn Cameras: A Policy Scorecard (US)

To increase the transparency and accountability of body-worn cameras, the Leadership Conference on Civil and Human Rights & Upturn in the United States developed a tool to assess and structure the information that can be extracted from footage filmed by body-worn cameras.

The tool proposes eight criteria to assess such footage:

1. Whether the footage is made public and readily available by the police department.

2. Whether officers' discretion on when to record is clearly disclosed.

3. Whether privacy concerns are addressed.

4. Whether officers must review the footage before drafting their initial written report.

5. Whether unflagged footage should be deleted within a predefined period.

6. Whether footage is protected against tampering and misuse.

7. Whether footage is made available to individuals filing complaints.

8. Whether the use of biometric technologies to identify individuals in the footage is limited or not.

Such initiatives can help to reinforce accountability by setting standards and encouraging the implementation of mechanisms to assess whether footage is collected and used appropriately.

For more information, see the Leadership Conference on Civil and Human Rights & Upturn, website on the policy scorecard.
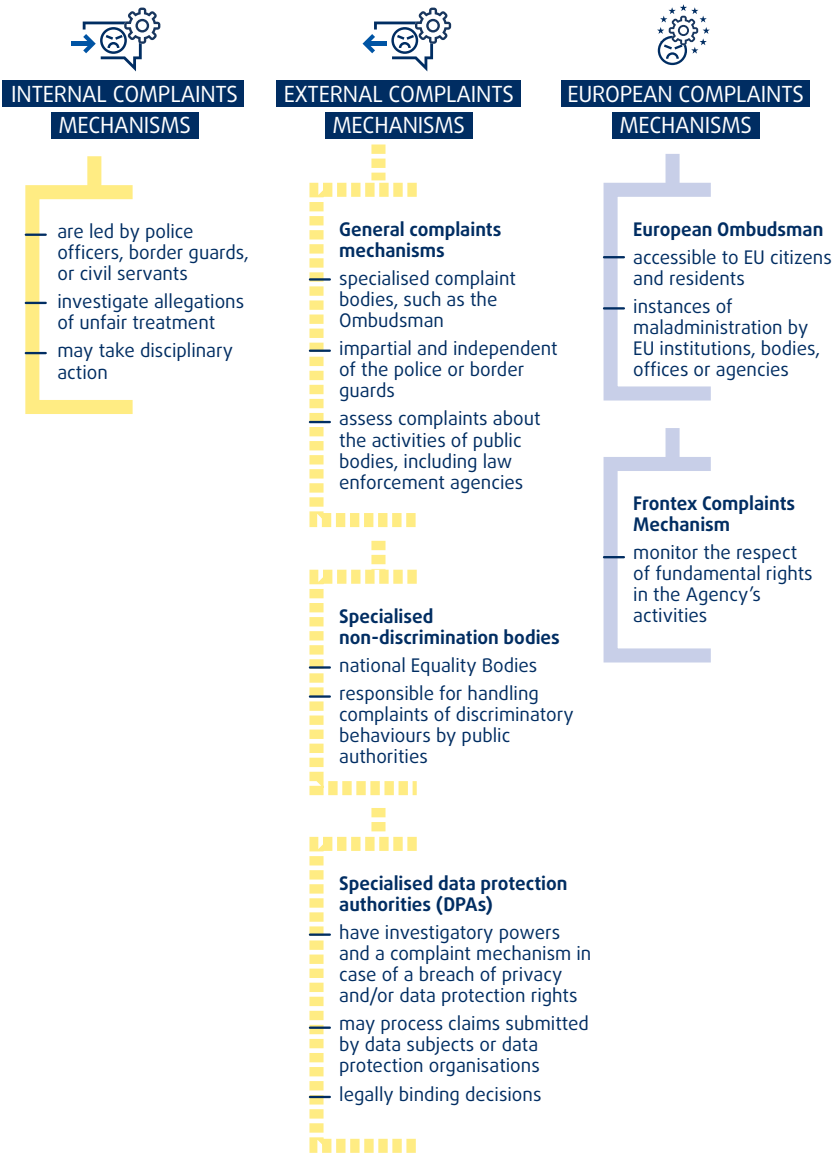
2.3.3. Complaints mechanisms

Effective complaints mechanisms can both deter abuses of power and help secure and restore public trust in the operations of police and border management authorities. They usually exist alongside formal legal channels that allow individuals to challenge the action or decision of a public authority before an independent and impartial tribunal.

To be effective, it is essential that:

- **Individuals can easily access complaint mechanisms**: evidence consistently shows that people are reluctant to make complaints, for example because the process is long or expensive, or because they fear negative repercussions. Making complaints mechanisms easily accessible through the use of online platforms such as websites or apps may encourage people to use them. In addition, organisations can support individuals in bringing complaints, either by bringing complaints on their behalf or through collective redress mechanisms, as envisaged in Article 80 (2) of the GDPR.

- **Complaints are handled transparently**: this will help increase confidence in complaints mechanisms.

- **Complaints bodies are independent** of the organisation, or the part of the organisation against which the complaint is brought.

There are a wide range of different mechanisms which handle different types of complaints. Figure 12 gives an overview of some of the complaints mechanisms available in EU Member States and at the EU level.

Figure 12: Overview of complaints mechanisms in EU Member States

INTERNAL COMPLAINTS MECHANISMS

— are led by police officers, border guards, or civil servants
— investigate allegations of unfair treatment
— may take disciplinary action

EXTERNAL COMPLAINTS MECHANISMS

General complaints mechanisms
— specialised complaint bodies, such as the Ombudsman
— impartial and independent of the police or border guards
— assess complaints about the activities of public bodies, including law enforcement agencies

Specialised non-discrimination bodies
— national Equality Bodies
— responsible for handling complaints of discriminatory behaviours by public authorities

Specialised data protection authorities (DPAs)
— have investigatory powers and a complaint mechanism in case of a breach of privacy and/or data protection rights
— may process claims submitted by data subjects or data protection organisations
— legally binding decisions

EUROPEAN COMPLAINTS MECHANISMS

European Ombudsman
— accessible to EU citizens and residents
— instances of maladministration by EU institutions, bodies, offices or agencies

Frontex Complaints Mechanism
— monitor the respect of fundamental rights in the Agency's activities

Source: FRA, 2018

Mechanisms where police officers come together with members of the public to listen to their complaints, discuss profiling and gain feedback for their operations provide an opportunity to learn important lessons to improve the processes that regulate profiling. They also create a means for involving the public in law enforcement activities (see case study).

Case study

Public complaint mechanisms in the law enforcement sector

Public Scrutiny Panels (West Midlands Police – United Kingdom)

Each of the eight Policing Boroughs within West Midlands Police (WMP) holds a bi-monthly Stop and Search Scrutiny Panel meeting, which is chaired by members of the public. These panels assess stop and search records, ensure that WMP respects the law, and give communities a channel to communicate complaints and raise issues of concern. The agendas and minutes of the meetings are published online. WMP has adopted a number of additional practices relating to community involvement in an effort to make street stops fairer and more targeted, and officers more accountable.

For more information, see West Midlands Police, webpage on stop and search and Her Majesty's Inspectorate of Constabulary (2016).

Reasonable Grounds Panels (Northamptonshire Police – United Kingdom)

Northamptonshire Police have put in place Reasonable Grounds Panels to involve members of the public in improving its stop and search operations. These panels are a channel for discussion on the use of stop and search powers and their impact on communities. They are chaired by a chief inspector and composed of a frontline officer and two members of the community, who can include offenders or ex-offenders. As well as enhancing communication between the police and the public, the panel has the authority to strip powers from officers and refer them for additional training to improve their stop and search operations.

For more information, see the Northamptonshire Police's webpage on the panel and Open Society Justice Initiative (2018a).

Informal network of police complaints mechanisms

The Independent Police Complaints Authorities' Network (IPCAN) is an informal network for exchange and cooperation amongst independent structures in charge of external control of security forces. It was created in 2013 and brings together complaints authorities from around 20 countries. These bodies, mainly from EU Member States, receive and process complaints against public security forces and, sometimes, against private ones.

For more information, see IPCAN's website*.*

In border management, public complaint mechanisms may be implemented through on the spot or *ex post* possibilities to lodge a complaint. The possibility to access such mechanisms increases transparency and accountability, and fosters mutual respect and good relationships between border guards and the public. The option to lodge a complaint *ex post* to a superior body rather than (only) directly at the border crossing point creates a degree of oversight and may positively influence the willingness of travellers to report possible incidents.[36]

Case study

Public complaint mechanisms in border management

Internal complaint mechanism at Manchester airport (United Kingdom)

At Manchester airport, the Central Allocation Hub provides a single point of contact for all passengers who wish to make a complaint. Complaints can be filed by email, letter, phone or fax, or face-to-face, and in English or Welsh. United Kingdom Border Force guidance outlines possible ways of resolving complaints. Minor misconduct such as rudeness, brusqueness or poor attitude can usually be resolved locally. Options include clarifying the issues with the customer, explaining operating procedures, agreeing further action and offering an apology if appropriate. Complaints about serious misconduct are usually assigned to the Professional Standards Unit. The Border Force guidance includes a test for determining signs of possible discrimination, which would constitute serious misconduct. If there is strong initial evidence

---

36   FRA (2014b).

that a passenger's treatment can be explained by factors other than race, the case is usually referred for local resolution.

For more information, see FRA (2014a), p.74.

Frontex Individual Complaint Mechanism (EU)

Following the adoption of the new Regulation of the European Border and Coast Guard Agency (Frontex) in 2016, Frontex established an individual complaints mechanism to monitor the respect of fundamental rights in the Agency's activities. These include pilot projects, return operations, joint operations, rapid border interventions, migration management support team deployments and return interventions. Any person whose rights have been directly affected by the actions of staff, including staff of national public authorities, involved in such Frontex activities can submit a complaint to the Frontex Fundamental Rights Officer. He or she decides on its admissibility and sends it to the Frontex Executive Director, as well as to the authorities of the affected Member State, if national staff were involved in the alleged violation. The complaint can be submitted in any language, by email, letter or via an online complaint form available on the Frontex website: http://frontex.europa.eu/complaints/.

Focus on the rights of law enforcement officers

Police officers are entitled to the same rights and freedoms as other persons, and are protected by human rights standards when performing their jobs. They can refer to their rights as laid down in various international human rights documents, such as: the European Convention on Human Rights (ECHR) or the International Covenant on Civil and Political Rights (ICCPR). The European Code of Police Ethics clarifies that "[p]olice staff shall as a rule enjoy the same civil and political rights as other citizens. Restrictions to these rights may only be made when they are necessary for the exercise of the functions of the police in a democratic society, in accordance with the law, and in conformity with the European Convention on Human Rights." One exception can be found in Article 11 of the ECHR, which refers to the right to freedom of assembly and association.

When carrying out police functions, especially when applying police powers, a police officer is not acting as a private individual but as an organ of the state. The state's obligation to respect and protect human rights therefore has a direct

effect on the options a police officer has to respond to aggression. The rights of police officers, who might risk injury or death to fulfil their duties, must also be respected and protected, such as by providing protective equipment, carefully planning police operations or taking preventive measures. Restrictions to his/her rights might be necessary for the exercise of police functions but any such limitations must reflect the principle of proportionality. Given their particular role as a state organ, police might face a greater limitation of their rights than an 'ordinary citizen'. Taking the example of a demonstration turning violent, an 'ordinary citizen' might run away or seek help, whereas a police officer is obliged to protect the human rights of others and restore public order.

For more information, see FRA (2013).

3

Algorithmic profiling

Algorithmic profiling includes any step-by-step computerised techniques that analyse data to identify trends, patterns or correlations.[37] Through profiling, the individual is selected "based on connections with others identified by the algorithm, rather than actual behaviour" and "individuals' choices are structured according to information about the group", rather than according to their own personal choices.[38]

Algorithmic profiling can be an efficient way for border management and law enforcement organisations to use data to prevent, detect and investigate crime. However, the collection and processing of large data sets raises a number of fundamental rights concerns. In addition to the importance of avoiding discrimination, algorithmic profiling introduces new risks, particularly in relation to rights to privacy and data protection. This section first concentrates on these new risks. It then illustrates the fundamental rights challenges associated with the use of algorithmic profiling in large-scale databases for border management and security purposes, and suggests some ways to minimise these risks.

---

37   For more information on what algorithms are, see FRA (2018b), p.4.

38   Mittelstadt, BD., Allo, P., Taddeo, M., Wachter, S. and Floridi, L. (2016).

Focus on predictive policing

Several software applications for predicting when and where a crime will be committed are used by law enforcement authorities. Some examples are: PredPol in the United Kingdom and the USA, the Criminality Awareness System (CAS) in the Netherlands, and Precobs in Germany and Switzerland. However, the effectiveness of these predictive methods for crime prevention has not yet been properly evaluated. Evidence so far shows contradictory findings, as the following examples show.

Predictive policing field test in Kent (UK) and Los Angeles (USA)

Police in the UK and US conducted an experiment to compare – against a more traditional approach – a fully automated algorithm for the identification of crime hotspots and the ensuing planning of police patrols.

Findings showed that the automated algorithm better identified future crimes. It predicted between 1.4 and 2.2 times more criminal actions than a crime analyst using traditional criminal intelligence and crime mapping practices. Moreover, patrolling actions based on the predictive tool are more effective, leading to an average reduction of 7.4 % in the number of crimes.

For more information, see Mohler, G.O., et al. (2016).

PILOT (Predictive Intelligence Led Operational Targeting) programme at Shreveport (USA)

This programme uses a predictive model to identify small areas at increased risk of property crimes and implement an intervention model in those areas to prevent property crimes. Results from three districts using PILOT were compared to three districts where traditional policing was conducted. There was no statistical evidence of a greater reduction in property crimes in the three PILOT districts examined.

For more information, see Hunt, P. et al (2014).

Beware software (USA)

'Beware' provides officers answering emergency calls with colour-coded scores (red, yellow, and green) indicating the threat level of the person or location involved. The software searches databases including arrest reports, property records, commercial databases, in-depth web searches, social media posts, and other publicly available databases.

The strengths and weaknesses of this system have not been evaluated. However, the lack of oversight of the decision-making process and the secretive nature of the algorithm, which is protected by trade secrets, have raised concerns about accountability. In addition, the potential inaccuracy of the data collected, and/or the information inferred from the analysis, may reduce the overall effectiveness of the tool.

For more information, see American Civil Liberties Union (2016).

Case study

Assessing impacts and risk of predictive policing – the ALGO-CARE assessment tool

The potential negative effects of the use of predictive policing must be taken into account to ensure a balanced and transparent overview of its impact on society. Analysis conducted by a group that included academics and police officers concluded that, as predictive policing is still in an experimental phase in the United Kingdom, detailed assessments of its impact on society and individuals are required. The research argues that there are some decisions which could have too great an impact on society and individuals for them to be influenced by an emerging technology; these cases should be removed from the influence of algorithmic decision-making.

The group developed a decision-making framework called ALGO-CARE for the deployment of algorithmic assessment tools in the policing context. This framework aims to guide police officers when assessing the potential risks of using predictive policing. It also attempts to translate key public law and human rights principles into practical considerations and guidance that can be addressed by public sector bodies.

The assessment tool invites police officers to assess the use of predictive policing through eight complementary steps:

- **Advisory**: to assess the extent of human intervention.
- **Lawful**: to assess the legal justification for using the algorithm.
- **Granularity**: to assess whether the algorithm can enter into sufficient level of detail on the specific case.
- **Ownership**: to ensure that the police force has the legal ownership and technical capacity to access, maintain, update and correct the source code on a regular basis.
- **Challengeable**: to ensure that oversight and audit mechanisms are in place.
- **Accuracy:** to assess whether the algorithm matches the policing aim, can be validated periodically and that the likelihood and impact of inaccuracy represents an acceptable risk.
- **Responsible:** to assess the fairness, accountability and transparency of the algorithm.
- **Explainable:** to assess the accessibility of information regarding both the decision-making rules and the impact that each factor has on the final outcome.

For more information, see Oswald, M., et al. (2017).

3.1. The data protection framework governing algorithmic profiling

The development and increasing use of new technologies – including the growing use of large data sets to support decision-making – prompted the EU to extensively revise its rules governing the processing of personal data in 2016. The two new instruments, the General Data Protection Regulation (GDPR) and the Police Directive, set out important principles and standards covering any decision based on comput-erised decision-making processes, including algorithmic profiling.

The GDPR and Police Directive entered into force in May 2018, meaning that there are few practical examples of implementation at the time of writing. Section 1.2.2

describes the legal standards governing the rights to privacy and data protection, and explains some of the main differences between the GDPR and the Police Directive (see Table 2). This chapter builds on this information to describe and explain the legal requirements concerning algorithmic profiling introduced by the GDPR and the Police Directive. These include:

- Data must be processed for a specific purpose based on a specific legal basis.

- Individuals must be informed when their personal data is processed.

- Data must be kept safe.

- Unlawful data processing must be detected and prevented.

Police officers and border guards requiring additional information on the legal requirements described in this chapter should turn to the data protection officers in their organisations. In addition, the *Handbook on European Data Protection Law* developed by FRA, the EDPS and the Council of Europe offers further guidance on the application of the Police Directive and the GDPR.[39]

Key points

- Algorithmic profiling must be **legitimate**, **necessary** and **proportionate.**
- Data shall not be processed without a **specific purpose based on a specific legal basis.**
- Individuals have specific rights described in detail in the provisions of the GDPR and the Police Directive, including:
  - **the right to be informed,** including to receive meaningful information on the logic involved in the algorithm,
  - the right **to access their personal data,**
  - the right **to lodge a complaint** with a supervisory authority, and
  - the right to an **effective judicial remedy.**
- Data should be **safely** collected, processed and stored.
- Unlawful data processing must be **prevented** and **detected.**

---

39   FRA, EDPS and Council of Europe (2018).

3.1.1. Data must be processed for a specific purpose

Any processing of personal data must have a legal basis. This means that it must be conducted to achieve **a specific purpose** set up in law.

Before any processing happens, an officer must know its purpose. This could include, among others:

• Is the data processed to detect a criminal offence?

• Is it processed to maintain public security?

• Is it processed to counter terrorism?

Once the purpose is correctly identified, officers will know which legal framework applies and the relevant legal obligations. Table 4 sets out how to identify which legal framework applies.

Table 4:   Identifying the correct legal framework depending on the purpose of processing

1. What is the purpose of data processing?	
• **prevention, investigation, detection or prosecution of criminal offences;** • **execution of criminal penalties;** • **safeguarding public security.**	• any other purpose
2. Police Directive applies	**2. General Data Protection Regulation applies**
3. Union or national law defines*	**3. Processing is only allowed when it is either:**
• **what personal data can be processed;** • **the specific purposes of the data processing.**	• **consented** to by the personal data subject; • necessary for the performance of a **contract**; • necessary to comply with **legal obligations**; • necessary to protect the **vital interests** of a person; or • necessary for the **public interest**.

4. Is the purpose of profiling exempt from the Police Directive?	4. Is the purpose of profiling exempt from the GDRP?
The rights to be informed, to access personal data, and to request the modification or erasure of the day may be limited (wholly or partially) in the following cases:	The obligations (to be transparent, to inform and to notify breaches) and rights (to access, rectify, erase, object or not to be subject to automated decision-making) set out in the GDPR **may be restricted** by national or EU law to safeguard:
• to avoid obstructing official or legal **inquiries**, investigations or procedures;	• national security, defence or public security;
• to avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;	• 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;
• to protect public security;	• 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 a matters, public health and social security;
• to protect national security;	
• to protect the rights and freedoms of others.	• the protection of judicial independence and judicial proceedings;
	• the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions;
	• a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the specific cases;
	• the protection of the data subject or the rights and freedoms of others;
	• the enforcement of civil law claims.

Note: *National acts transposing the Police Directive are available on Eur-Lex's website.
Source: FRA, 2018

3.1.2.   Individuals must be informed

Article 13 of the Police Directive and Articles 13 and 14 of the GDPR require that individuals be informed when their personal data are processed. Table 5 describes how and when to communicate information to the person whose data are being processed.

Table 5: Obligation to provide individuals with profiling information: type of data, means of communication and exceptions

Notification obligation - Checklist	
To whom?	Person whose data are processed
How?	• clear and plain language • easily accessible form • in the same form as the request – *prefer electronic means*
What?	**About the processing**: • your authority's name and contact details • your data protection officer's contact details • the purposes of the processing • the legal basis of the processing • the maximum period for storing the data • the types of persons/organisations that will receive the data **About the individuals' rights**: • the right to **lodge a complaint** with a supervisory authority and the contact details of the supervisory authority • the right to request **access** to his/her personal data • **rectification** and/or **erasure** of personal data • the right to request the **restriction** of the processing
Exceptions	• For excessive (i.e. repetitive) or manifestly unfounded requests • When the identity of the requester cannot be clearly confirmed • When communicating information would obstruct investigations • When communication of information would prejudice prevention/investigation of criminal offences • To protect public or national security • To protect the rights of other individuals

Source: FRA, 2018

Focus on the 'right to explanation'

In cases of profiling, the GDPR requires that "meaningful information about the logic involved, as well as the significance and the envisaged consequences" of the data processing be provided to the individual. This should be provided both when the data is collected (notification), and if the individual requests further information (right of access). This right is not explicitly mentioned in the Police Directive. However, recital 38 specifies that "[automated processing] should be subject to suitable safeguards, including the provision of specific information to the data subject […] in particular […] to obtain an explanation of the decision reached after such assessment or to challenge the decision".

This 'right to explanation' may prove difficult to implement in practice. Some individuals may have the digital literacy to understand the code of an algorithm, while for others, simplified information on the purpose of the processing and the interconnections of the data used is sufficient. The key to assessing the meaningfulness of the explanation provided is its objective. An individual should receive sufficient information to understand the purpose, the rationale and the criteria that led to a decision being made.

The right to an explanation is not absolute (see step 4 of Table 4). Member States may restrict this right by law in several cases, including: national security; defence; public security; the prevention, investigation, detection or prosecution of criminal offences; the execution of criminal penalties; the protection of the data subject or the rights and freedoms of others; or the enforcement of civil law claims.

Providing reasonable information on the purpose and envisaged consequences of the processing is nonetheless an advisable good practice. Developing simple ways to explain the logic involved and the criteria used to reach a decision will ultimately enhance transparency and accountability.

For more information, see GDPR, Articles 13 to 15 (right to information and right of access), Article 22 (automated individual decision-making, including profiling), and Article 23 (restrictions); and the Police Directive, Article 11 (automated individual decision-making, including profiling), and Articles 13 to 15 (right to information and right of access).

See also Article 29 Data Protection Working Party (2018a).

3.1.3. Keep the data safe: records, logs and storage rules

Authorities collecting and processing personal data for profiling purposes must not only process data lawfully, but ensure that data are not:

- accessed by unauthorised persons,

- used for other purposes than the original purpose, or

- stored for longer than necessary.

To this end, authorities and law enforcement boarder management officers must ensure that appropriate measures are implemented to protect the integrity and security of the data. They must keep track of any access to, and use of, the data by creating and maintaining records of all processing activities or categories of processing activities (Article 30 of the GDPR and Article 24 of the Police Directive). Records must contain:

- the **name** and **contact details** of the authorities and data protection officer;

- the **purpose** of the processing;

- the **categories of recipients** to whom the personal data have been or will be disclosed;

- a description of the categories of data subjects and of the categories of personal data;

- the **use of profiling**;

- an indication of the **legal basis** for the processing operation;

- where possible, the envisaged **time limits** for erasure of the different categories of personal data;

- where possible, a general description of the technical and organisational security measures referred to in Article 32 (1) of the GDPR or Article 29(1) of the Police Directive.

In addition, when computer-based profiling is implemented for purposes covered by the Police Directive (see Section 3.2), authorities must keep logs of the: collection, alteration, consultation, disclosure, including transfers, combination and erasure of data.

These records and logs will support officers in demonstrating their compliance with legal requirements during internal and external monitoring. If an individual makes a complaint, for instance, law enforcement and border management authorities will be required to make the records and logs available to national data protection authorities.

Personal data should not be stored for longer than necessary to achieve the established legitimate purpose. Storage for longer periods must be properly justified. In such cases, authorities should ensure that the storage is regularly reviewed to guarantee its integrity and security.

3.1.4.   Unlawful processing must be detected and prevented

Detecting and preventing unlawful processing of personal data is challenging. The specialist skills necessary to understand complex algorithms and large databases make it difficult to ensure proper checks.

To address this, the GDPR and Police Directive include safeguards to guide law enforcement and border management officers before, during and after the processing of data. These refer to:

• data protection impact assessments, and

• data protection by design and by default.

Impact assessments

The EU legal framework requires police and border management authorities to conduct impact assessments before conducting any data processing that is likely to result in a high risk to individuals' rights (Article 35 of the GDPR and Article 27 of the Police Directive). This means that impact assessments shall be conducted not only when the result of the processing may violate data protection or privacy standards,

but in any situation that may result in a violation of *any fundamental right*. This can include the rights to: equality and non-discrimination; freedom of expression and information; freedom of thought, conscience and religion; education; healthcare; asylum; and protection in the event of removal, expulsion or extradition. Impact assessments are particularly important where profiling may result in legal consequences for individuals. In such cases, the GDPR and the Police Directive require that impact assessments are conducted.

Impact assessments must be conducted prior to the automated processing itself. The objectives of these impact assessments are, however, twofold:

- *a priori*: before processing the data, conducting an impact assessment on the quality of the data and/or the algorithm behind the processing will help detect and, where relevant, remedy potential fundamental rights violations.

- *a posteriori*: once the data are processed, the officer may be required to demonstrate that he/she acted lawfully. The impact assessment may support him/her in proving that all necessary measures to ensure compliance with the law were implemented.

Impact assessments will also support officers in detecting hidden biases that may violate the rights to data protection and non-discrimination, and have an impact on the quality of the profiling (see Section 1.3.2).

Focus on the risks of the use of 'dynamic algorithms'

'Dynamic algorithms' are algorithms that are constantly redefined and 'improved' based on 'feedback loops'. These loops are created by the algorithmic systems themselves and cannot be properly understood or even expressed in simple language (see Article 35 of the GDPR and Article 27 of the Police Directive). Unlike 'static algorithms', which are based on predetermined criteria, 'dynamic algorithms' generate **new correlations** by constantly redefining themselves.

Dynamic algorithms create the risk that expert programmers will, at some point, no longer know the logic behind the algorithm. This creates a significant **risk of involuntarily reproducing existing prejudices** and of perpetuating social inequalities and the stigmatisation of certain groups. In

such cases, it becomes very difficult to ensure accountability and redress for the individuals concerned.

The use of 'dynamic algorithms' should therefore be **avoided or reduced** to minimise the risk of losing track of the assessment criteria. This enables internal and external auditors to evaluate the algorithms, and modify them if they are found to be unlawful. If the use of dynamic algorithms is justified, risk indicators shall be reviewed and tested to ensure that they do not result in unlawful profiling.

For more information, see Gandy, O. (2010) and Korff, D. (2015).

An impact assessment may vary significantly depending on the type and volume of personal data processed, and the type and purpose of the processing. It may include checking the quality of the data, technical controls of the algorithm(s) processing the data, and/or a complete review of the objectives of the processing, etc. Figure 13 sets out the minimum criteria that should be assessed.

The Article 29 Data Protection Working Party (now replaced by the European Data Protection Board), which brings together national data protection authorities in EU Member States, developed guidelines providing further information on data protection impact assessments. The guidelines include a detailed mapping of the criteria to use when conducting impact assessments.[40]

Embedding lawfulness 'by design' and 'by default'

Irrespective of whether or not an impact assessment detected the possibility for a fundamental rights violation, measures can be implemented to further prevent any risk of unlawfulness. These are referred to as 'Data protection by design' and 'Data protection by default' (Article 25 of the GDPR and Article 20 of the Police Directive).

Data protection by design aims to ensure that, both *before* and *during* the processing of data, technical and organisational measures are implemented to guarantee data protection principles. For instance, where feasible, personal data could be 'pseudonymised'. Pseudonymisation is a measure by which personal data cannot be linked to an individual without additional information, which is kept separately.

---

40   Article 29 Working Party (2017a).

Figure 13: Minimum requirements of impact assessments

1 Description of the profiling processing	2 Necessity and proportionality	3 Risks	4 Remedy
— What is the **purpose** of this profiling? — What are the envisaged processing **operations**? — What is the **legitimate interest** to conduct such profiling?	— In relation to the purpose established under 1, is such profiling **necessary** and **proportionate**? — Is such profiling the **least intrusive technique** to realise the purpose effectively?	— What **fundamental rights** may be impacted by this profiling? — What is the **scale** of the impact on individuals?	— What **measures** were taken to prevent, and/or remedy such risks? These may include safeguards, IT security measures, etc. — Would these measures be sufficient to **demonstrate compliance** with the law?

Source: FRA, 2018

The 'key' that enables re-identification of the individual must be kept separate and secure.[41] Contrary to anonymised data, pseudonymised data are still personal data, and therefore must respect data protection rules and principles.

Data protection by default ensures that "only personal data which are necessary for each specific purpose of the processing are processed".[42] This has an impact on:

- the amount of personal data collected and stored;

- the types of processing that may involve personal data;

- the maximum storage period;

- the number of persons authorised to access such personal data.

---

41   FRA, EDPS and Council of Europe (2018), p. 83.

42   General Data Protection Regulation (GDPR), Art. 25.

Focus on accountability

The primary objective of data protection by design and the data protection by default is to support law enforcement and border management authorities and officers to design algorithmic profiling programmes that comply with fundamental rights requirements, in particular the principles of **lawfulness**, **transparency** and **security**.

However, such measures may also demonstrate how authorities comply with the legal requirement of **accountability**. Authorities processing data are legally expected to implement "appropriate technical and organisational measures" to demonstrate their compliance with EU law. For example, if an individual makes a complaint, authorities may be requested by national judicial and data protection authorities to demonstrate each of these points:

- The legitimacy, necessity and proportionality of the computer-based profiling.

- The lawfulness of the purpose.

- The information provided to individuals.

- The integrity and security of the data.

- The quality measures and controls performed before and during the profiling operations.

3.2. Large-scale databases for border management and security purposes

The EU has developed several large-scale IT systems or mechanisms for the collection and processing of data that can be used for border and migration management and, to some extent, for law enforcement purposes. They serve as examples to illustrate some of the common challenges linked to the use of algorithmic profiling, as well as possible safeguards.

Table 6 briefly presents these EU IT-systems and mechanisms. The Annex gives a detailed overview of existing and planned EU large-scale IT systems, as of March 2018.

Table 6: Selected EU instruments involving the processing of large amounts of data for border management and law enforcement

Database	Acronym	Main Purpose
Schengen Information System	*SIS II*	Enter and process alerts on wanted or missing persons for the purpose of safeguarding security, enter and process alerts on third county nationals (TCNs) for the purpose of refusing entry or stay, and enter and process alerts on TCNs subject to a return decision.
Visa Information System	*VIS*	Facilitate the exchange of data between Schengen Member States on visa applications.
European Dactyloscopy	*EURODAC*	Determine the Member State responsible for examining an application for international protection and assist with the control of irregular immigration & secondary movements.
Entry/Exit System	*EES*	Calculate and monitor the duration of authorised stay of TCNs and identify over-stayers.
Passenger Name Record	*PNR*	Collect, process and exchange extra-EU flights passenger data of flights from third countries ('extra-EU flights').* Strictly speaking used only for law enforcement purposes.
Advanced Passenger Information	*API*	Collect and process passenger data of flights from third countries ('extra-EU flights') for border management and law enforcement purposes.
European Travel Information and Authorisation System	*ETIAS*	Assess if a visa-free TCN poses a security, irregular migration, or public health risk.
European Criminal Records Information System on Third Country Nationals	*ECRIS-TCN*	Share information on previous convictions of TCNs.

Note: ** In addition, Article 2 of Directive (EU) 2016/681 gives the Member States the option to process data from intra-EU flights.*

Source: *FRA, 2018*

EU large-scale IT systems are used in a number of migration-related processes, including: the pre-arrival risk assessment process, the asylum process, the visa application process, during border checks, when issuing residence permits, when apprehending migrants in an irregular situation, during return procedures and for issuing entry bans. IT systems set up by the EU, including those initially created for

asylum and migration management purposes, are also increasingly being used in the internal security context, such as for police checks and in the fight against serious crimes and terrorism.

Most of the systems set up by EU law focus on identifying a specific person by matching alphanumeric or biometric data (currently, fingerprints) with information already in the system. With some notable exceptions (see 'Focus on algorithmic profiling in EU instruments'), they do not themselves contain an algorithm that would allow a person to be matched with a profile. They can nevertheless be used to produce anonymised statistics, including on characteristics which are considered protected grounds, such as sex or age (see Section 1.2.1).

Such statistics could be used to set up risk profiles applied in future border management or policing decisions. As part of the wider scheme for the interoperability of EU IT systems, the European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (eu-LISA) will be responsible for managing the Central Repository for Reporting and Statistics. This repository will draw on data from existing EU databases (Entry/Exit System, ETIAS, Schengen Information System and Visa Information System) to generate statistics and analytical reports for EU and national bodies.[43]

Focus on algorithmic profiling in EU instruments

Some existing EU instruments foresee the use of statistics derived from their data to generate risk profiles. Besides allowing the detection of 'known' specific suspects, they contain an algorithmic profiling functionality which identifies 'unknown' individuals who may be of interest to law enforcement and border management authorities.

---

43 European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (borders and visa) and amending Council Decision 2004/512/EC, Regulation (EC) No 767/2008, Council Decision 2008/633/JHA, Regulation (EU) 2016/399 and Regulation (EU) 2017/2226*, COM(2017) 793 final, Strasbourg, 12 December 2017; European Commission (2017), *Proposal for a Regulation of the European Parliament and of the Council on establishing a framework for interoperability between EU information systems (police and judicial cooperation, asylum and migration)*, COM(2017) 794 final, Brussels, 12 December 2017.

The **European Travel Information Authorisation System (ETIAS)**,[44] adopted in September 2018 but not yet in operation at the time of the finalisation of this guide, will assess whether visa-exempt third-country nationals present a risk in terms of irregular migration, security or public health before granting the travel authorisation. Information provided by travellers during the application process will be automatically compared with relevant EU and international databases, and a set of risk indicators ('screening rules') contained in the ETIAS system itself. An algorithm developed by Frontex will compare the individual profile of the traveller (based on indicators such as age, sex, nationality, place of residence, education level and occupation) with these risk indicators to determine whether the application should be referred to a manual review.

Passenger Name Record (PNR) data are collected by air carriers from the information provided by passengers in flight reservation systems, such as travel dates and itinerary, contact and payment details, baggage information and other 'general remarks' such as dietary preferences. There is no central EU database collecting this data, but the EU PNR Directive[45] requires air carriers to provide the data to the national Passenger Information Units (PIUs), which then analyse the information for the purpose of combating terrorism and serious crime. Besides detecting the cross-border movement of known persons, these data can be used to identify as yet unknown threats by processing passengers' data against specific risk indicators ('pre-determined criteria'). These criteria are set by the PIUs and updated based on new data and patterns available in the system.

3.2.1. Minimising the fundamental rights risks of processing data in large-scale databases

Comprehensive data on travellers such as nationality, sex and age, will be used for profiling, including algorithmic profiling, at a scale which was not possible in the past. Even if these data are anonymised, their processing does not come without risk. Conscious or unconscious bias in the selection of risk indicators, design of the

---

44   European Commission (2018), *Regulation (EU) 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System (ETIAS) and amending Regulations (EU) No 1077/2011, (EU) No 515/2014, (EU) 2016/399, (EU) 2016/1624 and (EU) 2017/2226*, COM(2016) 731 final, Brussels, 16 November 2016, Art. 33(5).

45   *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*, OJ L 119, Art. 6(4).

algorithms or interpretation of the results could lead to operational actions which could result in discrimination of certain categories of persons.[46]

This section looks at some of these risks, and proposes some ways to minimise them. It builds on FRA's *Twelve operational fundamental rights considerations for law enforcement when processing PNR data* (see case study). While developed in the specific context of PNR data processing, some of these considerations are more generally applicable, and can be considered as safeguards mitigating the risks arising from algorithmic profiling.

Case study

FRA operational guidance for setting up national PNR systems

In 2014, in the absence of EU PNR legislation, the European Commission requested FRA to provide practical guidance relating to the processing of PNR data for law enforcement purposes for those Member States planning to set up their own national PNR schemes. The guidance focused on the rights to respect for private life (Article 7 of the Charter), protection of personal data (Article 8 of the Charter) and non-discrimination (Article 21 of the Charter). Some of the proposed safeguards were later introduced into the EU PNR Directive.

The twelve fundamental rights' considerations for law enforcement when processing PNR data are:

- Use PNR data only to combat terrorism and serious transnational crimes.

- Limit access to the PNR database to a specialised unit.

- Do not request direct access to airlines' databases.

- Delete sensitive PNR data.

- Set strict security and traceability safeguards against abuse.

- Reduce likelihood of flagging false positives.

- Be transparent towards passengers.

- Allow persons to access and rectify their PNR data.

---

46   For more information, see FRA (2017e), and FRA (2018a).

- Do not permit identification of data subjects or retention of data for longer than necessary.

- Transfer data extracted from PNR only to competent national public authorities.

- Only transfer data extracted from PNR to third countries under strict conditions.

- Carry out objective and transparent evaluation of the PNR system.

For more information, see FRA (2014c).

Processing of data revealing protected characteristics should be necessary and proportionate

The nature of algorithmic profiling means that the use of personal characteristics that are related to protected grounds entails a particularly high risk of discrimination.[47] In the EU context, both ETIAS and PNR legislation prohibit basing risk indicators on criteria that entail a high risk of discrimination, including race, ethnic origin or religious beliefs. However, even in the absence of such data, other types of data can be strongly correlated with these characteristics, effectively acting as proxies for such protected characteristics. For example, the category 'general remarks' of PNR, possibly containing travellers' dietary preferences, could reveal certain religious beliefs.

A specific combination of data used by the algorithm may also put a category of persons at a disadvantage. For example, it may disadvantage persons due to their ethnic or social origin or membership of a national minority, which are protected characteristics under Article 21 of the Charter. For instance, if a risk profile in ETIAS concerning the risk of irregular migration is based on the combination of a certain nationality and occupational group, it may result in targeting an ethnic group or nationality which in a certain country typically works in a particular economic sector, such as construction or agriculture.[48]

- Processing of data revealing characteristics protected by Article 21 of the Charter should be limited to what is strictly necessary and proportionate, and never result in discrimination. Before any processing, the competent authority should

---

47   European Data Protection Supervisor (2018).

48   See also FRA (2017a).

assess the data to identify any protected characteristics and remove any data, the processing of which would not be lawful. As a good practice, this should be complemented by running a matching and removal program with a regularly updated glossary of "sensitive terms".

Profiling criteria should be specific and targeted

Another risk results from the use of **broad profiling criteria**. Existing EU instruments allow significant discretion for the development of profiling algorithms. To assess the risk of irregular migration, ETIAS envisages the use of EU and national statistics on the rate of overstays and refusals of entry. For security risks, however, it only generally refers to information concerning specific security indicators and threats. The PNR Directive offers general indications for designing algorithms but does not specify what criteria to use to identify persons potentially involved in a terrorist offence or serious crime, or what weight to assign to a specific criterion.

Excessively broad criteria lead to a significant number of 'false positives', meaning that persons are wrongly matched with a certain risk profile. Some of these 'false positives' might also be discriminatory in nature. For example, a broad definition of the criterion 'past criminal conviction' means that LGBT individuals would be required to report criminal records associated with certain sexual conduct criminal-ised by some non-EU countries.

- Assessment criteria should be pre-defined, targeted, specific, proportionate and fact-based. Assessment criteria should be tested on anonymised samples. They should be subject to regular reviews by an internal auditor to determine whether they are still justified by their specific objectives.

- Before transmitting an alert based on automated processing for further action, the competent authority should manually review the data in conjunction with other information to determine whether the person matches the risk profile and eliminate false positives. Data recipients should provide feedback on the action taken on the basis of the alert.

Data processed should be accurate and reliable

FRA's research confirms that existing large-scale IT-systems contain a significant amount of inaccurate data.[49] **Inaccurate or unreliable data** may have multiple negative effects in the context of algorithmic profiling for border management or law enforcement purposes. Inaccurate data may adversely affect individuals but also lead to incorrect correlations and a distorted picture, compromising the effectiveness of police and border management work.

This is particularly relevant in cases of data entered by members of the public, as in the PNR data and ETIAS applications, that may be more prone to mistakes than official records. Similarly, screening social media accounts, which is foreseen by some travel authorisation systems outside the EU, entails a high risk of introducing unreliable information into the profiling process. In addition, it carries a particular risk of collecting information revealing sensitive personal information protected by the Charter, such as political opinion or information relating to sexual life.

- Provide accurate information to individuals on the collection, storage and processing of their data and on the applicable data protection principles. Individuals should be made aware of their rights, including the redress mechanisms available to them.

- Allow persons to seek to rectify their data where the data are inaccurate, and to be informed whether the data have been rectified or erased.

- Provide effective administrative and judicial redress in case any data protection rights have been violated, including if access has been denied or inaccurate data have not been rectified or erased.

---

49   See FRA (2018c), pp. 81-98.

Conclusion

Profiling is a legitimate tool used by law enforcement officers and border guards to prevent, investigate and prosecute criminal activity, as well as to prevent and detect irregular immigration.

To be lawful, fair, and effective, profiling must be used within the boundaries of the law. In particular, profiling must respect equal treatment and personal data protection requirements.

This will be achieved by a combination of elements. Any profiling should:

• treat individuals equally, respectfully and with dignity;

• avoid profiling individuals based on bias;

• be reasonable, objective, and intelligence-led; and

• adequately protect individuals' personal data and private life.

Different tools are available to police officers and border guards to ensure that these principles are known, understood, and upheld in practice:

• before conducting profiling, officers should receive guidance and training;

• during profiling, details of the activity should be recorded and stored;

• after profiling, officers' actions should be monitored and assessed to identify areas for improvement.

Preventing unlawful profiling will not only keep law enforcement officers and border guards within the law, it will ensure that their actions are understood and accepted by the general public. Boosting trust and confidence in law enforcement and border management improves the effectiveness of policing and border management, and therefore contributes to increasing safety and security levels in society as a whole.

Annex

Table 7: Existing and planned EU large-scale IT systems

IT system	Main purpose	Persons covered	Applicability	Legal instrument / proposal	Biometric identifiers
European dactylography (Eurodac)	Determine the Member State responsible for examining an application for international protection *Assist with the control of irregular immigration and secondary movements*	Applicants and beneficiaries of international protection, *Migrants in an irregular situation*	28 EUMS + SAC	Regulation (EU) No. 603/2013 (Eurodac Regulation) *COM(2016) 272 final (Eurodac proposal)*	
Visa Information System (VIS)	Facilitate the exchange of data between Schengen Member States on visa applications	Visa applicants and sponsors	24 EUMS (not CY, HR, IE, UK)[1] + SAC	Regulation 767/2008/EC (VIS Regulation)	
Schengen Information System (SIS II) - police	Safeguard security in the EU and Schengen Member States	Missing or wanted persons	26 EUMS (not CY, IE)[2] + SAC	Council Decision 2007/533/JHA (SIS II Decision) *COM(2016) 883 final (SIS II police proposal)*	
Schengen Information System (SIS II) - borders	Enter and process alerts for the purpose of refusing entry into or stay in the Schengen Member States	Migrants in an irregular situation	25 EUMS (not CY, IE, UK)[2] + SAC	Regulation 1987/2006 (SIS II Regulation) *COM(2016) 882 final (SIS II borders proposal)*	
Schengen Information System (SIS II) - return	*Enter and process alerts for third-country nationals subject to a return decision*	*Migrants in an irregular situation*	*25 EUMS (not CY, IE, UK)[2] + SAC*	*COM(2016) 881 final (SIS II return proposal)*	

Entry-Exit System (EES)	*Calculating and monitoring the duration of authorised stay of third-country nationals and identifying over-stayers*	*Travellers coming for a short-term stay*	*22 EUMS (not BG, CY, HR, IE, RO, UK)[3] + SAC*	*Regulation (EU) 2017/2226 (EES Regulation)*	
European Travel Information and Authorisation System (ETIAS)	*Assess if a visa-free third-country national poses a security, irregular migration or public health risk*	*Visa free travellers*	*26 EUMS (not IE, UK)[3] + SAC*	*COM(2016) 731 final (ETIAS proposal)*	*None*
European Criminal Records Information System for Third Country Nationals (ECRIS-TCN)	*Share information on previous convictions of third-country nationals*	*Third-country nationals with a criminal record*	*27 EUMS (not DK)[4]*	*COM(2017) 344 final (ECRIS-TCN proposal)*	
Interoperability – Common Identity Repository	*Establish a framework for interoperability between EES, VIS, ETIAS, Eurodac, SIS II and ECRIS-TCN*	*Third-country nationals covered by Eurodac, VIS, SIS II, EES, ETIAS and ECRIS-TCN*	*28 EUMS[5] + SAC*	*COM(2017) 793 final (Borders and visa inter-operability proposal) COM(2017) 794 final (Police coop-eration, asylum and migration interoperability proposal)*	

Note: *Planned systems and planned changes within systems are in italics, or shown by a light blue background.*

 Fingerprints; *Palm prints;* *Facial image;* *DNA profile.*

EUMS: EU Member States; SAC: Schengen Associated Countries, i.e. Iceland, Liechtenstein, Norway and Switzerland.

[1]   *Ireland and the United Kingdom do not participate in VIS. Denmark is not bound by the Regulation but has opted in for VIS. VIS does not yet apply to Croatia and Cyprus, and only partially applies to Bulgaria and Romania as per Council Decision (EU) 2017/1908 of 12 October 2017.*

[2]   *Cyprus and Ireland are not yet connected to SIS. Denmark is not bound by the Regulation or the Council Decision but has opted in for the SIS II, and must decide whether to opt in again upon the adoption of the SIS II proposals. The United Kingdom is participating in SIS but cannot use or access alerts for refusing entry or stay into the Schengen area. Bulgaria, Croatia and Romania cannot issue Schengen-wide alerts for refusing entry or stay in the Schengen area as they are not yet part of the Schengen area.*

[3]   *Denmark may decide to opt in for EES and ETIAS.*

[4]   *ECRIS-TCN does not apply to Denmark. The United Kingdom and Ireland may decide to opt in.*

[5]   *Denmark, Ireland and the United Kingdom will take part as they participate in the IT systems made interoperable.*

Source: *FRA, based on existing and proposed legal instruments, 2018*

References

Akhgar, B., Saathoff, G.B., Arabnia, H.R., Hill, R., Staniforth, A. and Bayerl, P. S. (2015), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies"*, Butterworth-Heinemann, 2015.

American Civil Liberties Union (ACLU) (2016), *Eight Problems With Police "Threat Scores",* 13 January 2016.

Article 29 Data Protection Working Party (2014), *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 536/14/EN, WP 211, Brussels, 27 February 2014.

Article 29 Data Protection Working Party (2017a), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, 4 October 2017.

Article 29 Data Protection Working Party (2017b), *Opinion on some key issues of the Police Directive (EU 2016/680)*, 7 December 2017.

Article 29 Data Protection Working Party (2018a), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP251 rev.01, 6 February 2018.

Article 29 Data Protection Working Party (2018b), *Opinion on Commission proposals on establishing a framework for interoperability*, WP266, Brussels, 23 April 2018.

Belgium, Unia, *Annual Report 2016*, Brussels, September 2017.

Belgium, Unia, *Rapport annuel Convention entre Unia et la police fédérale, Budget 2015*, Brussels, 2015.

Big Brother Watch, Smile you're on body worn camera Part II – Police, The use of body worn cameras by UK police forces, August 2017.

Body-Gendrot, S. (2016), 'Making sense of French urban disorders in 2005', *European Journal of Criminology*, Vol. 13, No. 5, pp. 556–572.

Bovens et al. (2014), 'Public accountability' in: Bovens, M., Schillermans, T. and Goodlin, R.E. (eds.), *The Oxford handbook of public accountability*, Oxford, Oxford University Press, 2014.

Brayne, S. (2014), 'Surveillance and system avoidance: criminal justice contact and institutional attachment', *American Sociological Review*, Vol. 79, No. 3, pp. 367–391.

Buolamwini, J., Gebru, T. (2018), *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, MIT Media Lab and Microsoft Research, 2018.

Centre d'analyse stratégique (2006), *Enquête sur les violences urbaines - Comprendre les émeutes de novembre 2005 : les exemples de Saint-Denis et d'Aulnay-Sous-Bois*, Paris, La Documentation française, 2006.

Center on Privacy and Technology at Georgetown Law (2016), *The Perpetual Line-up, Unregulated Police Face Recognition in America*, 18 October 2016.

Coudert, F, Butin, D. and Le Metayer, D. (2015), 'Body-worn cameras for police accountability: opportunities and risks', *Computer Law and Security Review*, Vol. 31, pp. 749–762.

Council of Europe, Committee of Ministers (2001), Recommendation Rec(2001)10 of the Committee of Ministers to Member States on the European Code of Police Ethics adopted by the Committee of Ministers, 19 September 2001.

Council of the European Union (2009), *Updated EU Schengen Catalogue on External borders control, Return and readmission*, 19 March 2009.

De Hert, P. and Lammerant, H. (2016), 'Predictive profiling and its legal limits: effectiveness gone forever?' in: van der Sloot, B., Broeders, D. and Schrijvers, E. (eds.), The Netherlands Scientific Council for Government Policy, *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, pp. 145–173.

Défenseur des droits (2017), Enquête sur l'accès aux droits. Volume 1 – relations police/population: le cas des contrôles d'identité, 2017.

Dinant, J.-M., Lazaro, C., Poullet Y., Lefever, N. and Rouvroy, A. (2008), *Application of Convention 108 to the Profiling Mechanism - Some ideas for the future work of the consultative committee (T-PD),* Doc. T-PD 01, p. 3.

European Border and Coast Guard Agency (FRONTEX) (2012), *Common core curriculum, EU border guard basic training*, March 2012.

European Border and Coast Guard Agency (FRONTEX) (2013), *Fundamental rights training for border guards, Trainers' Manual*, 2013.

European Border and Coast Guard Agency (FRONTEX) (2015), *Twelve seconds to decide. In search of excellence: Frontex and the principle of best practice*, 2015.

European Border and Coast Guard Agency (FRONTEX) (2017), *Handbook on risk profiles on Trafficking in Human Beings*, 2017.

European Commission (2017a), *Hate crime training for law enforcement and criminal justice authorities: 10 key guiding principles*, February 2017.

European Commission (2017b), *Improving the recording of hate crime by law enforcement authorities, Key guiding principles*, December 2017.

European Commission against Racism and Intolerance (ECRI) (2007), *ECRI General Policy Recommendation N° 11 on combating racism and racial discrimination in policing adopted on 29 June 2007*, Strasbourg, 4 October 2007.

European Commission, Subgroup on methodologies for recording and collecting data on hate crime (2017), *Improving the recording of hate crime by law enforcement authorities - Key guiding principles*, Brussels, December 2017.

European Data Protection Supervisor (EDPS) (2015), *Second Opinion on the Proposal for a Directive of the European Parliament and of the Council on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, Opinion 5/2015*, Brussels, 24 September 2015.

European Data Protection Supervisor (EDPS) (2018), *Opinion 4/2018 on the Proposals for two Regulations establishing a framework for interoperability between EU large-scale information systems*, Brussels, 18 April 2018.

European Monitoring Centre on Racism and Xenophobia (2016), *Perceptions of discrimination and islamophobia – Voices from members of Muslim communities in the European Union*, 2006.

European network of legal experts in gender equality and non-discrimination (2016), *Links between migration and discrimination - A legal analysis of the situation in EU Member States*, July 2016.

European Union Agency for Fundamental Rights (FRA), European Data Protection Supervisor (EDPS) and Council of Europe (2018), *Handbook on European data protection law – Edition 2018*, Luxembourg, Publications Office, May 2018.

Farrar, T. (2018), *Self-awareness to being watched and socially-desirable behavior: A field experiment on the effect of body-worn cameras on police use-of-force*, Police Foundation, 2018.

FRA (European Union Agency for Fundamental Rights) (2013), *Fundamental rights-based police training – A manual for police trainers*, Luxembourg, Publications Office, December 2013.

FRA (2014a), *Fundamental rights at airports: border checks at five international airports in the European Union*, Luxembourg, Publications Office, 2014.

FRA (2014b), *Fundamental rights at land borders: findings from selected European Union border crossing points*, Luxembourg, Publications Office, 2014.

FRA (2014c), *Twelve operational fundamental rights considerations for law enforcement when processing Passenger Name Record (PNR) data*, February 2014.

FRA (2016), *Fundamental Rights Report 2016*, Luxembourg, Publications Office, 2016.

FRA (2017a), *Opinion of the European Union Agency for Fundamental Rights on the impact on fundamental rights of the proposed Regulation on the European Travel Information and Authorisation System (ETIAS)*, FRA Opinion – 2/2017 [ETIAS], June 2017.

FRA (2017b), *Second European Union Minorities and Discrimination Survey - Main results*, Luxembourg, Publications Office, December 2017.

FRA (2017c), *Fundamental Rights Report 2017*, Luxembourg: Publications Office, May 2017.

FRA (2017d), *Second European Union Minorities and Discrimination Survey: Muslims – Selected findings*, Luxembourg: Publications Office of the European Union, September 2017.

FRA (2017e), *Fundamental rights and the interoperability of EU information systems: borders and security*, Luxembourg, Publications Office, May 2017.

FRA (2018a), *Interoperability and fundamental rights implications – Opinion of the European Union Agency for Fundamental Rights*, FRA Opinion – 1/2018 [Interoperability], April 2018.

FRA (2018b), *#BigData: Discrimination in data-supported decision making*, FRA Focus Paper, May 2018.

FRA (2018c), *Under watchful eyes: biometrics, EU IT systems and fundamental rights*, Luxembourg, Publications Office, February 2018.

FRA (2018d), *Hate crime recording and data collection practice across the EU*, Luxembourg, Publications Office, June 2018.

FRA (2018e), *Fundamental Rights Report 2018*, Luxembourg, Publications Office, June 2018.

FRA and Council of Europe (2018), *Handbook on European non-discrimination law – 2018 edition*, Luxembourg, Publications Office, February 2018.

France, Ministry of Interior (2018), *Rapport d'évaluation sur l'expérimentation de l'emploi des caméras mobiles par les agents de police municipale*, 7 June 2018.

Harcourt, B. (2004), 'Rethinking Racial Profiling: A Critique of the Economics, Civil Liberties, and Constitutional Literature, and of Criminal Profiling More Generally', *University of Chicago Law Review*, Vol. 71, 2004.

Harris, D. (2002), 'Flying While Arab: Lessons from the Racial Profiling Controversy', *Civil Rights Journal*, Vol. 6, No.1, winter 2002.

Harris, D. (2003), *Profiles in Injustice; Why Racial Profiling Cannot Work*, The New Press, 2003.

Hildebrandt, M. and de Vries, K. (2013), *Privacy, due process and the computational turn: the philosophy of law meets the philosophy of technology*, New York, Routledge, 2013.

Hildebrandt, M. and Gutwirth, S. (eds.) (2008), *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Berlin, Springer, 2008.

Hörnqvist, M. (2016), 'Riots in the welfare state: The contours of a modern-day moral economy', *European Journal of Criminology*, Vol. 13, No. 5, pp. 573–589.

Hunt, P., Saunders, J. and Hollywood, J. S. (2014), *Evaluation of the Shreveport predictive policing experiment*, RAND Corporation, 2014.

Gandy, O. (2010), 'Engaging rational discrimination: exploring reasons for placing regulatory constraints on decision support system', *J Ethics Inf Technol*, Vol. 12, No. 1, pp. 29-42, 2010.

Gross, S. R. (2002), 'Racial Profiling under Attack', D. Livingston, co-author. *Colum. L. Rev.* 102, No. 5, pp. 1413-38.

Jobard, F. (2008), 'The 2005 French urban unrests: data-based interpretations', *Sociology Compass*, Vol. 2, No. 4, pp. 1287–1302.

Kádár, A., Körner, J., Moldova, Z., and Tóth, B. (2008), *Control(led) Group, Final Report on the Strategies for Effective Police Stop and Search (STEPSS) Project*, Budapest, p. 23.

Keskinen, S. et al (2018), *The Stopped – Ethnic Profiling in Finland*, Swedish School of Social Science, University of Helsinki, Helsinki, 3 April 2018.

Korff, D. (2015), *Passenger Name Records, data mining & data protection: the need for strong safeguards*, T-PD(2015)11, Strasbourg, 15 June 2015.

Miller, J. and Alexandrou, B. (2016), *College of policing stop and search training experiment: Impact evaluation*, College of Policing Limited, 2016.

Mittelstadt, BD., Allo, P., Taddeo, M., Wachter, S. and Floridi, L. (2016), 'The ethics of algorithms: Mapping the debate', *Big Data & Society*, 1 December 2016.

Mohler, G.O., Short, M. B., Malinowski, S., Johnson, M., Tita, G. E., Bertozzi, A.L., Brantingham, P.J., *Randomized Controlled Field Trials of Predictive Policing*, 15 January 2016.

Nisbet, R., Elder, J. and Miner, G. (2009), *Handbook of Statistical Analysis & Data Mining Applications*, Sydney (Canada), Elsevier, 2009.

Open Society Justice Initiative (2018a), *Regulating Police Stop and Search: An Evaluation of the Reasonable Grounds Panel*, December 2018.

Open Society Justice Initiative (2018b), *The Recording of Police Stops: Methods and Issues*, December 2018.

Oswald, M., Grace, J., Urwin, S. and Barnes, G., 'Algorithmic Risk Assessment Policing Models: Lessons from the Durham HART Model and 'Experimental' Proportionality', *Information & Communications Technology Law*, 31 August 2017.

Schauer, F. (2003), *Profiles Probabilities and Stereotypes*, Cambridge (MA), The Belknap Press of Harvard University Press, 2003.

Scheinin, M. (2007), United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism, *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, UN Doc. A/HRC/4/26, 29 January 2007.

The Guardian (2015), *Northamptonshire police ban stop and search by officers who abuse powers*, 18 August 2015.

The Office of the United Nations High Commissioner for Human Rights (OHCHR) (2014), *Recommended Principles and Guidelines on Human Rights at International Borders*, 23 July 2014.

Tóth, B.M. and Kádár, A. (2011), 'Ethnic profiling in ID checks by the Hungarian police', *Policing and Society*, Vol. 21, No. 4, pp. 383–394.

United Kingdom, Camden and London Prepared (2006), *Major Incident Procedures, What businesses and the voluntary sector need to know*, April 2006.

United Kingdom, College of Policing (2016), *Stop and Search*, Authorised Professional Practice (APP), 29 September 2016.

United Kingdom, Equality and Human Rights Commission (2009), *Police and racism: what has been achieved 10 years after the Stephen Lawrence Inquiry report?*, 2009.

United Kingdom, Her Majesty's Inspectorate of Constabulary (HMIC) (2013), *Stop and Search Powers: Are the police using them effectively and fairly?*, 2013.

United Kingdom, Her Majesty's Inspectorate of Constabulary (HMIC) (2016), *PEEL: Police legitimacy 2015 An inspection of West Midlands Police*, February 2016.

United Kingdom, Home Office (1999), *The Stephen Lawrence Inquiry. Report of An Inquiry by Sir William Macpherson of Cluny*, February 1999.

United Kingdom, Home Office (2014a), *CODE A: Revised code of practice for the exercise by: police officers of statutory powers of stop and search; police officers and police staff of requirements to record public encounters*, Norwich, The Stationery Office (TSO), 2014.

United Kingdom, Home Office (2014b), *Best use of stop and search scheme*, 2014.

United Kingdom, House of Commons Home Affairs Committee (2009), *The Macpherson Report – Ten Years On*, Twelfth Report of Session 2008–09, 22 July 2009.

United Kingdom, House of Lords (2006), *Opinions of the Lords of appeal for judgment in the cause R (on the application of Gillan (FC) and another (FC)) (Appellants) v. Commissioner of Police for the Metropolis and another (Respondents)*, [2006] UKHL 12, 8 March 2006.

United Kingdom, London School of Economics (2011), *Reading the Riots*, December 2011.

United Kingdom, National Policing Improvement Agency (NPIA) (2012), *Stop and search, the use of intelligence and geographic targeting, Findings from case study research*, 2012.

United Kingdom, Northamptonshire Police (2018), *Get Involved – Reasonable Grounds Panel*, accessed April 2018.

United Kingdom, Staffordshire PCC Matthew Ellis, Ethics, Transparency and Audit Panel (2015), *An Independent Report into Stop & Search Encounters by Staffordshire Police,* January 2015.

United Kingdom, Stop Watch (2011), *"Carry on Recording" Why police stops should still be recorded*, May 2011.

United Kingdom, West Midlands Police (2012), *Stop and Search Policy*, November 2012.

United Kingdom, West Midlands Police (2016), *Stop and Search Recommendations*, July 2015 (last amended June 2016).

United Kingdom, West Midlands Police (2017a), *Stop and Search in the West Midlands: Presentation to Den Hague City Council*, April 2017.

United Kingdom, West Midlands Police (2017b), *New "app" set to speed up Stop & Search process*, August 2017.

United Kingdom, West Midlands Police (2018), *Stop and Search Scrutiny Panels,* accessed on April 2018.

United Kingdom, West Midlands Police and Crime Commissioner (2014), *Stop and Search Action Plan – Outcome of consultation*, January 2014.

United Nations (UN) (2007), *Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism*, A/HRC/4/26, 29 January 2007.

USA, GAO (General Accounting Office) (2000), *U.S. Customs Office: better targeting of airline passengers for personal searches could produce better results,* GAO/GGD-00-38, March 2000.

Van Brakel, R. (2016), 'Pre-emptive big data surveillance and its (dis)empowering consequences: the case of predictive policing' in: van der Sloot, B., Broeders, D. and Schrijvers, E. (eds.), The Netherlands Scientific Council for Government Policy (*Wetenschappelijke Raad voor het Regeringsbeleid*), *Exploring the boundaries of big data*, Amsterdam, Amsterdam University Press, pp. 117–141.

Wrench, J. (2007), *Diversity management and discrimination: immigrants and ethnic minorities in the EU*, Aldershot, Ashgate, 2007.

Zarsky, T.Z. (2011), 'Governmental Data Mining and its Alternatives', *Penn State Law Review*, Vol. 11, No. 2, pp. 285–330.

EU legislation

Fundamental Rights

Charter of Fundamental Rights of the European Union, 2012/C 326/02, OJ 2012 C 326.

Explanations relating to the Charter of Fundamental rights, 2007/C 303/02, OJ 2007 C 303/17.

Non-discrimination

Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment.

Council Directive 2000/78/EC of 27 November 2000 establishing a general framework for equal treatment in employment and occupation.

Data Protection

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, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance).

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, and repealing Council Framework Decision 2008/977/JHA.

Border management

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second-generation Schengen Information System (SIS II), OJ 2007 L 205/63 *(SIS II)*.

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, OJ 2016 L 119/132.

Regulation (EC) No. 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation Schengen Information System (SIS II), OJ 1987 L 381/4.

Regulation (EC) No. 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas, OJ 2008 L 218/60 (*VIS Regulation*).

Regulation (EC) No. 603/2013 of the European Parliament and of the Council of 26 June 2013 on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) 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 and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes, and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice, OJ 2013 L 180/1.

Regulation (EU) No. 1624/2016 of the European Parliament and of The Council of 14 September 2016 on the European Border and Coast Guard and amending Regulation (EU) 2016/399 of the European Parliament and of the Council and repealing Regulation (EC) No 863/2007 of the European Parliament and of the Council, Council Regulation (EC) No 2007/2004 and Council Decision 2005/267/EC, OJ 2016 L 251/1.

Regulation (EU) No. 1052/2013 of the European Parliament and of the Council of 22 October 2013 establishing the European Border Surveillance System (Eurosur), OJ 2013 L 295/11.

Regulation (EU) 2016/399 of the European Parliament and of the Council of 9 March 2016 on a Union Code on the rules governing the movement of persons across borders (Schengen Borders Code).

Case Law

France, Court of Cassation (*Cour de Cassation*), *Décision 1245*, 9 November 2016.

United Kingdom, House of Lords, *R (on the application of Gillan et al.) v. Commissioner of Police for the Metropolis et al.,* [2006] UKHL 12, 8 March 2006.

CJEU, C-524/06, *Heinz Huber v. Bundesrepublik Deutschland*, 16 December 2008.

ECtHR, *B.S. v. Spain*, No. 47159/08, 24 July 2012.

ECtHR, *S. and Marper v. United Kingdom,* Nos. 30562/04 and 30566/04, 4 December 2008.

ECtHR, *Gillan and Quinton v. the United Kingdom*, No. 4158/05 2010, 12 January 2010.

UNHRC, *Rosalind Williams Lecraft v. Spain,* Comm. No. 1493/2006, 30 July 2009.

FRA

EUROPEAN UNION AGENCY
FOR FUNDAMENTAL RIGHTS

Technological developments have triggered an increased use of profiling in a wide range of contexts, and using profiling tools to support the work of law enforcement and border management officials has recently received greater attention from EU Member States. Profiling is legitimately used to prevent, investigate and prosecute criminal offences, as well as to prevent and detect irregular immigration. But unlawful profiling can undermine trust in the authorities and stigmatise certain communities.

This guide explains what profiling is, the legal frameworks that regulate it, and why conducting profiling lawfully is both necessary to comply with fundamental rights and crucial for effective policing and border management. The guide also provides practical guidance on how to avoid unlawful profiling in police and border management operations.

Information society

Internal security

Non-discrimination

Publications Office