PICUM BRIEFING

DATA PROTECTION AND THE FIREWALL: ADVANCING SAFE REPORTING FOR PEOPLE IN AN IRREGULAR SITUATION

PICUM
PLATFORM FOR INTERNATIONAL COOPERATION ON
UNDOCUMENTED MIGRANTS

Modern information technology and the age of Big Data have dramatically increased the likelihood of misuse of individuals' personal data. Recognising this, on 25 May 2018, the EU adopted the General Data Protection Regulation (GDPR), a powerful new legislative framework that reinforces everyone's right to the protection of their personal data by improving transparency and accountability in the processing of personal data and strengthening individuals' control over how their data is used.

The GDPR has particular relevance for migrants' rights given the growing large-scale use of data processing to enhance migration control and policing.[1]

This factsheet explains the relationship between the GDPR and the concept of the "firewall", a tool to safeguard the fundamental rights of people in an irregular situation in Europe.

Insecure Status Creates Vulnerability to Abuse and Exploitation

The criminalisation of migrants in an irregular situation reinforces vulnerability to victimisation. It leads authorities to prioritise the enforcement of immigration rules over rules protecting the rights of victims, resulting in increased risk of abuse, and limited recourse for victims with insecure status. In addition to triggering return procedures, in most member states irregular entry and stay are offences that are also separately punishable with imprisonment or fines. Measures criminalising various aspects of irregular migration have a disproportionate impact on minority communities.[2]

Perpetrators realise there are no consequences for their actions. Abusers can use a person's insecure status to control them, to convince them that they have no right to help, and to threaten deportation or separation from their families if they dare to report mistreatment. Being undocumented enhances unequal power dynamics that can be exploited. This is frequently true for women, whose residence status is often dependent to their spouse or partner, and who often work in highly informal sectors where their employment and their residence status are typically precarious and heavily dependent on a single employer.[3]

1 Statewatch (2019), Data Protection, Immigration Enforcement and Fundamental Rights: What the EU's Regulations on Interoperability Mean for People with Irregular Status.

2 EU Agency for Fundamental Rights (2014), Criminalisation of migrants in an irregular situation and of persons engaging with them.

3 United Nations Development Program (2018), A practitioner's toolkit on women's access to justice programming; M. LeVoy, 11 Nov 2017, Al Jazeera, "The women who fear saying #MeToo"

THE "FIREWALL" SAFEGUARDS FUNDAMENTAL RIGHTS AND PROMOTES THE SAFETY AND RIGHTS OF UNDOCUMENTED VICTIMS

"Firewalls" are built on the premise that while states have the prerogative to enforce immigration laws, they also have obligations to protect fundamental rights. Those fundamental rights include the right to access justice. A "firewall" delinks the provisions of key services, included those needed by people who have been victimised, from the enforcement of immigration rules, ensuring that public trust and community safety are not undermined or interfered with by political objectives on migration control.

Under international law, everyone has the right to non-discrimination and to a remedy if their rights are violated. These rights are reflected in the EU Charter of Fundamental Rights, in Articles 21 and 47, respectively.

EU law also sets out specific rights for people who have been the victim of a crime. Directive 2012/29/EU (Victims' Directive) establishes minimum standards on the rights of victims of crime.

The Victims' Directive addresses vulnerability linked to residence status

- The Victims' Directive must be applied to all victims, without discrimination, *"including with respect to their residence status"* (Article 1).
- The Directive recognizes that victims who are not nationals of the country where they were victimized are "*particularly vulnerable*" or at "*particularly high risk of harm*" (Recital 38).
- The Directive emphasises the need to address repeat forms of victimisation and acknowledges that people are more likely to report crime if they believe they will be treated respectfully and be taken seriously by the authorities (Recitals 9 and 63; Articles 1(1) and 2(1)).
- The Directive gives special attention to the needs of victims of gender-based violence and notes that women who are victims of such violence and their children often need special support and protection (Recitals 17, 38, 57 and Articles 9(1)(b), 22(3), 26(2)).

The "firewall", expressed in Article 1 of the Directive, restores priority to the rights of victims and the safety of communities in situations of vulnerability ahead of the enforcement of immigration rules. It means creating a legal, technical and organizational separation between public immigration enforcement activities targeted at people who are undocumented and service provision to the same individuals, in the areas of health care, social services, education and access to the justice system.

The EU General Data Protection Regulation (GDPR) provides additional, and complementary, standards that clarify and reinforce the rights of undocumented victims under the Victims' Directive.

Violence against Undocumented Women: Their right to safety, protection and justice

The rights of undocumented women are recognised and protected under international human rights law.

In August 2014, the **Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)** entered into force and became the first legally binding instrument providing a comprehensive legal framework to prevent violence against women, protect victims and end the impunity of perpetrators. The Convention applies to all women regardless of migration status (Article 4) and addresses the situation of women on spouse-dependent visas by requiring parties to make available independent residence permits to victims (Article 59). The explanatory report makes specific reference to women in an irregular situation and to the increased risk of violence they face, as well as the difficulties and structural barriers they confront in overcoming such violence. The report also specifically calls on states to provide safe accommodation in specialized women's shelters. In May 2015, an international group of independent experts, the GREVIO Committee, was established to monitor the Convention's implementation at the national level. As of December 2019, 22 EU member states were party to the Convention.

The **UN Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)** became effective in 1981 and has been ratified by every EU member state. The CEDAW Committee noted in its General Recommendation no. 33 (para. 10) that intersecting forms of discrimination limit access to justice, and that women "often do not report violations of their rights to the authorities for fear that they will be humiliated, stigmatised, arrested, deported, tortured or have other forms of violence inflicted upon them, including by law enforcement officials." The Committee has called on states to ensure women's "unhindered access to justice systems" without discrimination, as a condition of achieving equality. More recently, in General Recommendation 35 (para. 29), it has urged states to reform laws that "prevent or deter women from reporting gender-based violence", including "restrictive immigration laws."

GDPR: PROTECTION OF PERSONAL DATA REINFORCES THE "FIREWALL"

The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 and sets out clear rules on the processing of personal data that increase the rights of individual data subjects, with the aim of fostering greater transparency and accountability in the use of personal data. The GDPR applies across the European Economic Area (EEA) to the processing of data by private actors, certain authorities, and public service providers. The GDPR should be understand as an effort to strengthen even further fundamental rights to privacy, taking into account advancements in technology and the ease with which personal data can be collected and transmitted today.

Because irregular entry and stay are often criminalised, people who are undocumented face the risk that seeking help or trying to report mistreatment to the authorities will expose them to immigration enforcement. Explicit data-sharing arrangements between law enforcement and immigration services exists in some member states, which has the effect of discouraging victims with insecure status from coming forward, leading to repeat victimisation and impunity.

The GDPR reaffirms that data protection is a fundamental right under EU law that applies to everyone. The GDPR also reinforces important concepts linked to access to justice, such as the right to non-discrimination and to an effective remedy.

The GDPR:

- Imposes strict rules on the use of personal data by public authorities and private actors who are active within the European Economic Area.
- Further strengthens and implements fundamental human rights to privacy and data protection, and protects individuals' rights without distinction based on nationality, place of residence, or residence status.
- Is grounded in rights already well-established under the EU Charter of Fundamental Rights (Articles 7 and 8) and the European Convention on Human Rights (Article 8), born out of atrocities committed during WWII and privacy right infringements during the Cold War, and responds to concerns about new technology and the potential encroachment of big data on those rights.
- Arguably restricts the further sharing, transfer or exchange of personal data obtained from victims and witnesses, for immigration enforcement purposes.

The GDPR establishes several key Principles for the lawful processing of data.

Purpose limitation

The GDPR sets strict limits on the reasons for which data can be processed.

The principle of "purpose limitation" is a cornerstone of the GDPR, and of data protection rights under the European Court of Human Rights. It requires that personal data be collected for a specified, explicit and legitimate purpose, and not be further processed in a way incompatible with this purpose.

If information is originally collected by service providers or law enforcement authorities for the purpose of responding to a complaint by or outreach from victim or witness, its repurposing to engage in immigration enforcement against the victim or witness will likely be incompatible with the initial purposes for the processing – particularly given the private nature of the data and the potential far-reaching negative impact on an already vulnerable population of data subjects.

Data minimization

The GDPR prohibits processing of personal data beyond what is strictly needed to achieve the purpose for which the data was initially collected.

The principle of "data minimization" requires that personal data gathered must be adequate, relevant and limited to what is necessary in relation to the purpose for which it is collected.

Processing information about an individual's immigration status will generally not be necessary for the purpose of providing protection, services and support to a victim, or to following up on a complaint that has been lodged. Where it might be needed, for instance, because they might be eligible for specific protection measures, the purpose limitation must be respected.

Sensitive data

The GDPR provides enhanced protection for sensitive data. This includes data revealing racial or ethnic origin, or data concerning health, or residence status.

Such data, which can also include personal data concerning sex life or sexual orientation, and, in some cases, biometric or genetic data, should generally only be processed with the consent of the person or, in exceptional circumstances, when necessary for reasons of substantial public interest under national or EU law.

Exceptions to the GDPR are narrow, recognising that data protection and privacy rights are fundamental rights.

- Governments can only deviate from the GDPR based on clear EU or national legislation that: (i) respects the fundamental rights and freedoms of individuals who would be affected by the exception; (ii); safeguards a specific and pressing social need (such as national security, the prevention, investigation, detection or prosecution of criminal offences or other important objectives of general public interest); (iii) is sufficiently clear and precise to be foreseeable to affected individuals; and (iv) is necessary and proportionate in a democratic society.
- There is a strong case to make that immigration enforcement that interferes with access to essential services, such as health care, is unlikely to meet this high threshold.

RESOURCES

- Centre on Migration, Policy and Society (COMPAS), Oxford University, "Safe Reporting" of crime for victims and witnesses with irregular migration status in the USA and Europe (August 2018-October 2019).
- Committee on the Elimination of Discrimination against Women, General recommendation No. 33 on women's access to justice, CEDAW/C/GC/33, 23 July 2015.
- Committee on the Elimination of Discrimination against Women, General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, CEDAW/C/GC/35, 14 July 2017.
- Council of Europe, European Commission against Racism and Intolerance (March 2016), ECRI General Policy Recommendation No. 16 – On Safeguarding Irregularly Present Migrants from Discrimination.
- Liberty (2019), Care Don't Share: Hostile Environment Data-Sharing: Why We Need a Firewall Between Essential Public Services and Immigration Enforcement.
- PICUM Fact Sheet (November 2018), Achieving a world free from violence against women – What is the Istanbul Convention?
- PICUM (2015), Guide to the EU Victims' Directive: Advancing Access to Protection, Services and Justice for Undocumented Migrants.
- Regulation (EU) 2016/679 of the European Parliament and 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)

This publication was made possible with kind support from:

European Commission

This publication has received financial support from the European Union Programme for Employment and Social Innovation "EaSI" (2014-2020). For further information please consult: http://ec.europa.eu/social/easi

ADESSIUM FOUNDATION

Epim European Programme for Integration and Migration

OAK FOUNDATION

OPEN SOCIETY FOUNDATIONS

SIGRID RAUSING TRUST

The information contained in this publication does not necessarily reflect the official position of the European Commission.

Cover photo: Yanosh Nemesh, from Dreamstime