DATA PROTECTION AND THE “FIREWALL”: ADVANCING SAFE REPORTING FOR PEOPLE IN AN IRREGULAR SITUATION
The GDPR has particular relevance for migrants’ rights given the growing large-scale use of data processing to enhance migration control and policing.  

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.

The “FIREWALL” SAFEGUARDS FUNDAMENTAL RIGHTS AND PROMOTES THE SAFETY AND RIGHTS OF UNDOCUMENTED VICTIMS

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.

ECtHR also sets out specific rights for people who have been the victim of a 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 recognises that victims who are not nationals of the country where they were victimised are “particularly vulnerable” or are “particulary at risk of harm” (Recital 26).

» 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 (Recital 9 and Articles 1(1) and 2(1)).

» The Directive gives special attention to the needs of victims of gender-based violence and notes that women are victims of such violence and their children often need special support and protection (Recital 17, 36, 37, and Article 8(b), 23(2), 24(2)).

» The “FIREWALL” is recognised in Article 1.1 of the Directive.

The Directive requires the establishment of measures to protect the rights of victims and to avoid the safety of communications or diversion of vulnerability ahead of the enforcement of immigration rules. It makes creating a “firewall” in the form of a ‘firewall’, a ‘firewall’ between immigration enforcement activities targeted at migrant communities and interventions to protect the safety of victims and to enforce the right to access justice.

Insecure Status Creates Vulnerability to Abuse and Exploitation

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 their data.

The GDPR is a legal act that clarifies and reinforces the rights of undocumented people to access justice systems 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.

"Firewalls" or "firewalls" were built on the premise that while states have the prerogative to enforce immigration laws, they also have obligations to protect fundamental rights. These fundamental rights include the right to access justice. “Firewalls” divide the provisions of key services, including 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. A “firewall” delinks the provisions of key services, included those needed by people in an irregular situation in Europe.

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 across the European Economic Area (EEA) to the processing of data by private actors, certain authorities, and public service providers. The GDPR should be understood as an effort to strengthen even further fundamental rights to privacy, taking into account advancements in technology, and the use with which personal data can be collected and transmitted today.

The EU Data Protection Regulation (GDPR) came into force on 25 May 2018 and sets out clear rules on the processing of personal data, including those needed by people in an irregular situation in Europe.

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. 30 (para. 10) that intersecting forms of victimisation 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”. Achieving this is a condition of achieving equality. More recently, in its General Recommendation (15 pages, 20), it has urged states to refrain less that “prevent or deter women from reporting gender based violence” including “repressive immigration laws”.

In 2015, the Council of Europe Convention on preventing and combating violence against women and domestic violence (Council Convention) entered into force to help prevent violence against women, protect victims and sentence perpetrators. The Convention applies to all residents 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 face in accessing such services. The report also specifically calls on states to provide safe accommodation in specialised women’s shelters. In May 2015, an international group of independent experts, the OIUSCC Committee, was established to monitor the Convention’s implementation at the national level.

The European Union’s Fundamental Rights Agency noted in its annual report for 2017 that the EU should ensure that women in an irregular situation in Europe do not face barriers to their access to justice and the redress of harm due to violence against women.

In 2015, the Council of Europe Convention on preventing and combating violence against women and domestic violence (Council Convention) entered into force to help prevent violence against women, protect victims and sentence perpetrators. The Convention applies to all residents 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 face in accessing such services. The report also specifically calls on states to provide safe accommodation in specialised women’s shelters. In May 2015, an international group of independent experts, the OIUSCC 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.

In their General Recommendation no. 30 (para. 10) that intersecting forms of victimisation 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”. Achieving this is a condition of achieving equality. More recently, in its General Recommendation (15 pages, 20), it has urged states to refrain less that “prevent or deter women from reporting gender based violence” including “repressive immigration laws”.

The Treaty on the Functioning of the European Union (TFEU) confers on the EU powers in the fields of justice, fundamental rights, security, and Schengen cooperation.

The European Union’s Fundamental Rights Agency noted in its annual report for 2017 that the EU should ensure that women in an irregular situation in Europe do not face barriers to their access to justice and the redress of harm due to violence against women.

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.

The GDPR is a legal act that clarifies and reinforces the rights of undocumented people to access justice systems in the areas of health care, social services, education and access to the justice system. The GDPR provides additional, and complementary, standards that clarify and reinforce the rights of undocumented victims under the Victims’ Directive.

The 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 recognises that victims who are not nationals of the country where they were victimised are “particularly vulnerable” or are “particulary at risk of harm” (Recital 26).

» 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 (Recital 9 and Articles 1(1) and 2(1)).

» The Directive gives special attention to the needs of victims of gender-based violence and notes that women are victims of such violence and their children often need special support and protection (Recital 17, 36, 37, and Article 8(b), 23(2), 24(2)).

» The “FIREWALL” is recognised in Article 1.1 of the Directive.

The Directive requires the establishment of measures to protect the rights of victims and to avoid the safety of communications or diversion of vulnerability ahead of the enforcement of immigration rules. It makes creating a “firewall” in the form of ‘firewalls’ a ‘firewall’ between immigration enforcement activities targeted at migrant communities and interventions to protect the safety of victims and to enforce the right to access justice.

The Victims’ Directive also sets out specific rights for people who have been the victim of a 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 recognises that victims who are not nationals of the country where they were victimised are “particularly vulnerable” or are “particulary at risk of harm” (Recital 26).

» 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 (Recital 9 and Articles 1(1) and 2(1)).

» The Directive gives special attention to the needs of victims of gender-based violence and notes that women are victims of such violence and their children often need special support and protection (Recital 17, 36, 37, and Article 8(b), 23(2), 24(2)).

» The “FIREWALL” is recognised in Article 1.1 of the Directive.

The Directive requires the establishment of measures to protect the rights of victims and to avoid the safety of communications or diversion of vulnerability ahead of the enforcement of immigration rules. It makes creating a “firewall” in the form of ‘firewalls’ a ‘firewall’ between immigration enforcement activities targeted at migrant communities and interventions to protect the safety of victims and to enforce the right to access justice.

The Victims’ Directive also sets out specific rights for people who have been the victim of a crime.
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 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.


- 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?


- 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:

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

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

Cover photo: Yanosh Nemesh, from Dreamstime