DATA PROTECTION AND THE “FIREWALL”: ADVANCING THE RIGHT TO HEALTH FOR PEOPLE IN AN IRREGULAR SITUATION
Insecure Status Creates Health-Related Vulnerabilities

For people living in Europe with irregular status, being undocumented usually means being shut out from mental and physical health, which is exacerbated by extremely limited access to health care in most parts of Europe.

A person’s immigration status is changeable and dependent on many factors, particularly a country’s rules about the conditions of entry, and the risk of deportation, particularly in countries where public officials have a duty to report on irregular migrants. In addition to ensuring access to health care without discrimination, strict walls should exist between health-care personal and law enforcement authorities.1

THE “FIREWALL” SAFEGUARDS FUNDAMENTAL RIGHTS, INCLUDING THE RIGHT TO HEALTH

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 increases the right of individuals subject, with respect to their personal data, to have a duty to respect the right to health: Even where such formal arrangements don’t exist, there is often no protection against all has incidents of reporting by medical staff or administrators.

The GDPR reaffirms that data protection is a fundamental right under EU law that applies across the European Economic Area (EEA) to the processing of data by private persons, institutions, 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 need with which personal data can be collected and transmitted today.

A “firewall” delinks the delivery of health care from the enforcement of immigration rules, ensuring that public trust and the pursuit of important social and health goals are not undermined or interfered with by political objectives on migration control.1

The application of immigration rules must not interfere with the correct application of the human rights obligations of states in respect of all persons in their jurisdiction. There must be clear firewalls which separate the delivery of health care from immigration control and enforcement obligations.2

The GDPR protects the right to health by strengthening people's capacity to safeguard the fundamental rights that reinforce everyone's right to health – of people in an irregular situation in Europe.

A “firewall” ensures that while states have the prerogative to reform immigration laws, they also have obligations to protect fundamental rights. Those fundamental rights include the right to health.

The “firewall” reinforces the “firewall” a tool to safeguard the fundamental rights – including the right to health – of people in an irregular situation in Europe.
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 for the provision of health care, its transfer to immigration enforcement authorities will generally 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 public services like health care, education, or social services. Where it might be needed, for instance to verify eligibility for reimbursement of health costs, the purpose limitation must be respected.

- **Sensitive data**
  
  The GDPR provides enhanced protection for sensitive data. This includes data revealing racial or ethnic origin, data concerning health.

  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**

- 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 (2016), *The Sexual and Reproductive Health Rights of Undocumented Migrants: Narrowing the Gap between their Rights and the Reality in the EU.*
- 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*).