The EU’s new interoperability regulations will store the personal and biometric data of every EU citizen, from as young as 6 and retain personal records for up to 10 years, to facilitate the process of identification and verification. These databases create a linked database between existing migration and criminal law systems. The EU says this will improve its response to irregular migration and serious crimes like terrorism - but there is little evidence of the need or likely benefits of this approach, and a great risk of data abuse. These databases represent the growing use of integrated IT systems for immigration control and the EU’s new approach to irregular migration.

Data is collected at the national level by multiple authorities and stored in centralized EU servers.

- **Residence**
  - national
  - biometric
  - identity verification
- **Identity**
  - national
  - biometric
  - identity verification
- **Migration**
  - national
  - biometric
  - identity verification
- **Criminal**
  - national
  - biometric
  - identity verification

For some of the databases stored in centralised EU servers, the fingerprints of children as young as 6 are included.

We are not powerless. EU law includes strong provisions regulating the use of data. The EU General Data Protection Regulation (GDPR) applies to everyone in the EU, where their data is processed.

**GDPR**

- Applies to everyone in the EU whose data is processed (Article 5).
- Requires transparency and accountability in the processing of personal data (Article 1). The citizen has the right to know what type of personal data is collected and how it is processed.
- Grants data subject rights (Article 12): e.g. right to information, right of access, rectification and deletion.
- Requires the profiling of individuals (Article 22): e.g. to decide whether they are a threat.
- The EU Court of Human Rights, of which all EU countries are a party, guarantees the right to respect for privacy and family life (Article 8).

The protection and control of the use of data is one of the core values of the EU. The EU Court of Justice has held that the processing of personal data is necessary and proportionate in the EU (Case C-278/12 PPU Atiqullah Adil (2012)).

The new regulations contradict the EU’s longstanding approach to the protection of personal data as a fundamental right. Ignoring key principles of data protection, the new regulations are incompatible with the EU’s leadership on the protection of personal data.

The clear intention behind the new regulations is to make it easier to identify people in the EU without regular status, to make it easier to identify migrants and refugees, to identify criminal offenders, to monitor migration, to fight terrorism... all under the guise of fighting terrorism, degrading migrant communities.

Why is this approach so problematic?

- **Because it is discriminatory.**
  - The new regulations, and the revision new information systems they create, only apply to non-EU nationals. They are based on the discriminatory and unbalanced idea that non-EU nationals are more likely to engage in terrorist or criminal activities. These databases are only controlled by foreigners. They will only ever have an impact on foreigners.
  - The new approach undermines the EU’s longstanding commitment to non-discrimination.

- **Because it will deepen mistrust towards authorities among migrant communities.**
  - The clear intention behind the new regulations is to make it easier to identify people in the EU without regular status, to find a broader agenda of increased deportations. More identity checks will likely mean more discrimination and racial profiling, deepening migrant communities’ feeling of being over-policed and under-protected.

- **Because it is incompatible with the EU’s leadership on the protection of personal data.**
  - The new regulations contradict the EU’s longstanding approach to the protection of personal data as a fundamental right: crossing key principles of data protection. Interoperability blurs the line between databases that have historically served very different purposes, so that a copy of your passport stored today can be used later to facilitate your deportation.

How will interoperable migration systems affect people’s daily lives?

- **Travelling**
  - “The station several hours, worried and humiliated.”
  - Yassine is taken away for further questioning. He remains at the station for several hours, feeling of being over-policed and humiliated.
  - “Is he a citizen? Have you checked?”
  - The police assume Yassine is likely undocumented, because he does not appear in the CIR / common identity repository. The police stop them for a random check. They ask Yassine for his ID. He says he is a citizen, but only has a death certificate and identity fraud detector.

- **Identity**
  - “Is this your ID? We need to verify it.”
  - The police ask for his ID once again. He has a copy of his passport issued by the government.

- **Data protection**
  - “I think you can access this data in any case.”
  - “Is there a case for a court order?”
  - “There is no case.”

The EU’s new interoperability regulations will store the personal and biometric data of every EU citizen, from as young as 6 and retain personal records for up to 10 years, to facilitate the process of identification and verification. These databases create a linked database between existing migration and criminal law systems. The EU says this will improve its response to irregular migration and serious crimes like terrorism - but there is little evidence of the need or likely benefits of this approach, and a great risk of data abuse. These databases represent the growing use of integrated IT systems for immigration control and the EU’s new approach to irregular migration.

**Why is this approach so problematic?**

- **Because it is discriminatory.**
  - The new regulations, and the revision new information systems they create, only apply to non-EU nationals. They are based on the discriminatory and unbalanced idea that non-EU nationals are more likely to engage in terrorist or criminal activities. These databases are only controlled by foreigners. They will only ever have an impact on foreigners.
  - The new approach undermines the EU’s longstanding commitment to non-discrimination.

- **Because it will deepen mistrust towards authorities among migrant communities.**
  - The clear intention behind the new regulations is to make it easier to identify people in the EU without regular status, to find a broader agenda of increased deportations. More identity checks will likely mean more discrimination and racial profiling, deepening migrant communities’ feeling of being over-policed and under-protected.

- **Because it is incompatible with the EU’s leadership on the protection of personal data.**
  - The new regulations contradict the EU’s longstanding approach to the protection of personal data as a fundamental right: crossing key principles of data protection. Interoperability blurs the line between databases that have historically served very different purposes, so that a copy of your passport stored today can be used later to facilitate your deportation.

How will interoperable migration systems affect people’s daily lives?

- **Travelling**
  - “The station several hours, worried and humiliated.”
  - Yassine is taken away for further questioning. He remains at the station for several hours, feeling of being over-policed and humiliated.

- **Identity**
  - “Is this your ID? We need to verify it.”
  - The police assume Yassine is likely undocumented, because he does not appear in the CIR / common identity repository. The police stop them for a random check. They ask Yassine for his ID. He says he is a citizen, but only has a death certificate and identity fraud detector.

- **Data protection**
  - “I think you can access this data in any case.”
  - “Is there a case for a court order?”
  - “There is no case.”

What are people’s rights?

We are not powerless. EU law includes strong provisions regulating the use of personal data to ensure transparency and accountability, as well as individuals’ knowledge and control of what is done with their data. These are fundamental human rights that apply to everyone in the EU.