FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Responsible Digital Identity Management: Technologies for the Promotion of Data Protection

IDSF 2023

Ann-Charlotte Nygård, EU Fundamental Rights Agency (FRA)

Biometric identification: Why are fundamental rights, including protection of personal data, important?

Weak position of the individual:

- Identification and access to further information stored in EU IT-systems to support decision-making based on biometric data – fingerprints or facial image
- Data stored impact on future decision about the person
- May be perceived as untransparent
- People affected may not know how to claim their rights

Processing of biometric data involves fundamental rights risks

- Human dignity, prohibition of inhuman and degrading treatment:
  - Difficulties in fingerprinting interpreted as an attempt to avoid fingerprinting, and measures may possibly result in fundamental rights violations.
- Respect for private and family life:
  - Decisions affecting the future of the person taken based on false matches.
- Right to non-discrimination:
  - Difficulties in capturing quality biometrics – children, older people, people with disabilities, certain ethnicities.
- Right to asylum:
  - Biometrics is of decisive importance for the functioning of the Dublin system
- Rights of the child:
  - Children are in a particularly vulnerable situation.
- Etc.

…but also fundamental rights opportunities

- Right to liberty and security:
  - Prevention of identity fraud and theft.
- Rights of the child:
  - Enhanced protection of missing and abducted children.
- Right to asylum:
  - Help establishing the identity of asylum seekers without travel documents, which may contribute to the respect of the principle of non-refoulment.
- Etc.

Technically possible may not be legally possible…

What does EU data protection law say about using biometric data?

- Biometric data is categorised as a **special category of data, sensitive data**
- Processing of biometric data **is only allowed** where processing is **necessary** for reasons of substantial **public interest**, on the basis of **Union or Member State law** which shall be **proportionate** to the aim pursued, respect the **essence** of the right to data protection, and provide for **suitable and specific measures to safeguard** the fundamental rights and the interests of the **data subject**.

Source: General Data Protection Regulation (GDPR) Article 9

What does EU data protection law say about the use of personal data?

- The data protection principles of **purpose limitation and data minimisation** apply.

- Meaning that personal data should be collected only for **specific, explicit, and legitimate purposes.** The rules on access and use of the data should be limited to what is **necessary** for the objective, and the purpose be **foreseeable** for the person.

Source: General Data Protection Regulation (GDPR) Articles 5 and 6.

- Still, **risks**:
    - for function creep
    - for unauthorised access, unlawful further sharing, hacking

The example of interoperable IT-systems

- **Aim**: To detect multiple identities of non-EU nationals for security and immigration purposes.
- **Data access**: Specific biometric and biographical data are stored in the Common Identity Repository (CIR), plus references to the underlying information system holding data about the person. The user can access underlying the systems **only if already authorised to do so**. This includes access by law enforcement to fight **serious crime and terrorism**, but only for specific purposes and under strict conditions.
- **Police access for identification:** But **only if** no identity document, doubts about identity, refusal to cooperate, natural disasters, accidents, terrorist attacks.

  Safeguards:

  - National laws defining precise purpose, procedures, conditions and criteria, competent police authorities
  - Such laws to take into account the need to avoid discrimination
  - Biometrics taken live
  - Not allowed for children less than 12 years old, unless in the best interests of the child.

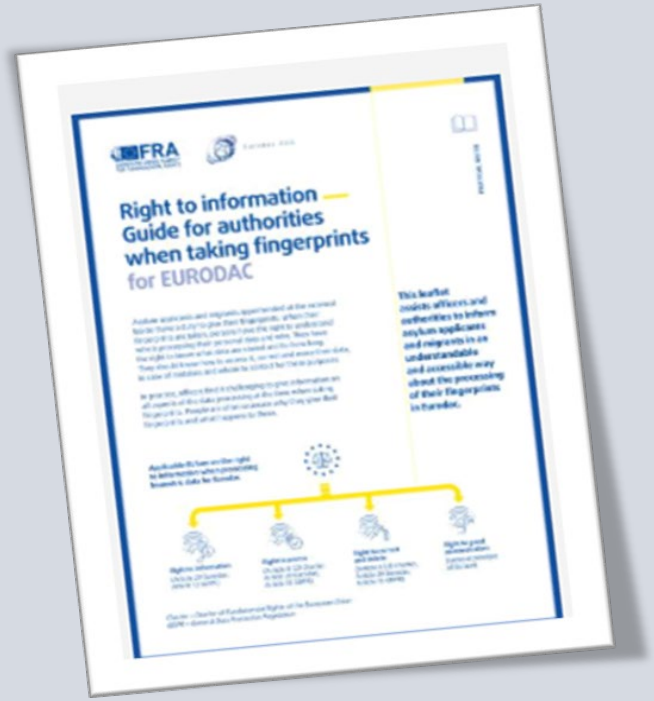
Source: Interoperability regulations (EU) 2019/817 and 2019/818

Rights of the child

- Children grow, reliability of fingerprints higher for children older than 12 years of age.
- Children are in a particularly vulnerable situation, for instance, a false match/non-match may impact on future decisions concerning them.
- Capture biometrics in a child-friendly and child sensitive manner.
- The best interest of the child shall always be the primary consideration

Right to an effective remedy

- **Right to information**:
  - On the purpose of the processing; where to lodge a complaint
- **Data subject's rights**:
  - Request for right of access, correction, and deletion of incorrect personal data
- **Judicial remedies**:
  - To ensure the rights of data subjects; claims for compensation due to unlawfulness



FRA EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Thank you!

FRA – EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

Schwarzenbergplatz 11 – 1040 Vienna – Austria

T +43 158030-0 – F +43 158030-699

facebook.com/fundamentalrights

twitter.com/EURightsAgency

linkedin.com/company/eu-fundamental-rights-agency

fra.europa.eu