HOW DO MEMBER STATES AND NORWAY ENSURE ACCURATE, TIMELY AND INTEROPERABLE DATA MANAGEMENT IN THE ASYLUM PROCEDURE?

EMN FLASH #18 – 2021

Introduction to the EMN study: Accurate, timely, interoperable? Data management in the asylum procedure

Recent years have seen changing circumstances in applications for international protection, with increases and decreases in the volume and types of applications, prompting procedural changes in the asylum process, impacting how personal data are collected, managed and shared in several Member States and Norway.

Most recently, the outbreak of the COVID-19 pandemic in early 2020 has also impacted on data management in asylum procedures.

How is data managed in the different phases of the asylum procedure? What do national approaches to data management look like, and what challenges do Member States face?

At a glance, the main research findings are introduced below.

Key findings

Member States collect different types of data as part of the asylum procedure. However, some categories of data are commonly collected by most, if not all, Member States and Norway, including data on current and/or birth names, birth date, citizenship, contact details, health status, photo and fingerprints, information on family members already in a Member State, vulnerabilities, and level of education.

A trend in frontloading data collection was observed for basic personal data (e.g. name, biometrics, place of birth) and supporting documents (e.g. passport and travel documents). As a result, an increasing amount of data is collected by border guards and local police, as the main authorities responsible for registering and lodging applications in most Member States.

Data on asylum applicants are primarily collected through oral interviews, questionnaires and electronic tools (for biometric data). However, several Member States have also started to use social media analysis, analysis of mobile devices and artificial intelligence (AI) to collect data on asylum applicants.

Most Member States and Norway cross-check data on asylum applicants against European (i.e. Visa Information System (VIS), Schengen Information System (SIS), Eurodac) and national databases.

EU data protection legislation requires Member States to have safeguards in place to ensure respect for the right to data protection. Member States and Norway have implemented several data safeguards in the asylum procedure, such as providing a privacy notice to applicants, assessing the quality of data collected in the asylum procedure, and implementing data protection supervisory and compliance mechanisms.

Since 2014, most Member States have experienced challenges in data management. These challenges primarily relate to the lack of human or financial resources and the interoperability of (national) databases.

Changes introduced by Member States in response to these challenges include **consolidating databases to increase interoperability, channelling asylum applications to prioritise certain cases, and implementing contingency measures to ease the asylum process in times of high numbers of applicants.**

Some Member States changed their data management procedures in response to challenges to the implementation of asylum processes posed by the COVID-19 pandemic, including the digitalisation of some steps of the asylum procedure and changes in the collection of fingerprints.

EMN
European Migration Network