ISSN 2600-514X

National cross-border digital tools and services in the field of EU social security coordination

ELA
EUROPEAN LABOUR AUTHORITY

When citing this report, please use the following wording:
European Labour Authority (2025), *National cross-border digital tools and services in the field of EU social security coordination*, ELA Report, Publications Office of the European Union, Luxembourg.

Editing and coordinating: David Arnoldussen, Slavomir Hidas and Vit Holubec (European Labour Authority).

Authors: Sophie Vancauwenbergh, Arianna Cantarelli and Giovanni Carletti, with the support of Inge Vandenbulcke, Willem Waeyaert, Sofia Falcone, Martin Andresen, Johan Magnusson and Juho Lindman.

The present document relies substantially on data and information collected by Milieu Consulting SRL and Eftheia. This task has been carried out exclusively by Milieu Consulting SRL and Eftheia in the context of a contract between them and the European Labour Authority (ELA), awarded following a tender procedure. The document has been prepared for ELA; however, it reflects the views of the authors only. The information contained in this report does not reflect the views or the official position of ELA.

Luxembourg: Publications Office of the European Union, 2025
Cover photo: @ wilaiwan - stock.adobe.com

PRINT: ISBN 978-92-9401-865-6 doi:10.2883/8947256 HP-01-24-004-EN-C
PDF: ISBN 978-92-9401-864-9 doi:10.2883/0445844 HP-01-24-004-EN-N

Contents

Lists of tables, figures and boxes

Abbreviations

Country codes

AT	Austria	**FI**	Finland	**LV**	Latvia
BE	Belgium	**FR**	France	**MT**	Malta
BG	Bulgaria	**HR**	Croatia	**NL**	Netherlands
CH	Switzerland	**HU**	Hungary	**NO**	Norway
CY	Cyprus	**IE**	Ireland	**PL**	Poland
CZ	Czechia	**IL**	Israel	**PT**	Portugal
DE	Germany	**IS**	Iceland	**RO**	Romania
DK	Denmark	**IT**	Italy	**SE**	Sweden
EE	Estonia	**LI**	Liechtenstein	**SI**	Slovenia
EL	Greece	**LT**	Lithuania	**SK**	Slovakia
ES	Spain	**LU**	Luxembourg	**UK**	United Kingdom

Other abbreviations

AI	artificial intelligence
API	application programming interface
AWOD	accidents at work and occupational diseases
CNAF	Family Benefit Funds (Caisse Nationale d'allocations familiales) (France)
CAK	Central Administration Office (Centraal Administratie Kantoor) (the Netherlands)
CSSA	Czech Social Security Administration
DC4EU	digital credentials for Europe
DDMS	digital document management system
DMA	digital maturity assessment
EBSI	European blockchain services infrastructure
EESSI	electronic exchange of social security information
EFTA	European Free Trade Association
EHIC	European health insurance card
eID	electronic identification
eIDAS	electronic identification and trust services
ELA	European Labour Authority
EOA	European Online Information Service (Germany)
ESSPASS	European social security pass
EU+	In the context of this study, the EU Member States, Iceland, Liechtenstein and Norway
EUDI	EU digital identity
GDPR	general data protection regulation
ICT	information and communications technology
IT	information technology

Kela	Social Insurance Institution of Finland
OECD	Organisation for Economic Co-operation and Development
ÖGK	Österreichische Gesundheitskasse (Austrian public health insurance fund)
PD	portable document
SDGR	single digital gateway regulation
TESS	telematics in social security
ZPIZ	*Pension and Disability Insurance Institute of Slovenia*

Executive summary

This report presents a mapping of digital tools and services for the purpose of cross-border social security coordination, covering the EU Member States plus Iceland, Liechtenstein and Norway ([1]). Drawing on desk research and qualitative interviews with national social security institutions, the study resulted in a comprehensive overview of how Member States are progressing in their digitalisation efforts within the social security sector, with a specific focus on the needs of mobile citizens and cross-border cases.

Assessments and analyses under this report do not cover exchanges through EESSI, but focus on parallel national-level initiatives. In the context of this report, interoperability is assessed outside EESSI for those areas/aspects that EESSI does not cover.

The report introduces a multidimensional framework for conceptualising and assessing digital maturity in cross-border social security. The analysis is therefore centred on five dimensions of digital maturity, tailored to social security coordination. The applied digital maturity assessment reveals the following factors:

- The user accessibility of social security services is improving, with online application platforms increasingly available for different social security branches in most Member States. Multilingual support and secure cross-border authentication are key areas for improvement.
- Digital administration is expanding across Member States. Automation tools have been introduced to support the processing of benefit claims and requests in many Member States, and digital documentation systems are becoming more widespread. However, cross-border cases often require manual intervention due to their complexity.
- As required by the EU rules on social security coordination, the Electronic Exchange of Social Security Information (EESSI system) ensures the exchanges of information between social security institutions across Europe, replacing paper-based communication. Interoperability of national systems outside EESSI is limited. Challenges in Member States exist regarding cross-border database integration.
- Network security and data protection is highly advanced, driven by robust EU regulation.
- Error and fraud detection is transforming through the use of digital strategies, with algorithms and digital tools developed to identify errors and potential cases of social security fraud.

Many Member States are advancing towards their common goal of digitalising the management and provision of social protection. The findings of this analysis show that digitalisation efforts beyond those required by EU legislation are primarily driven by institutions' and local specific needs, resulting in varied digital maturity levels across countries and social security branches. For instance, pension services exhibit high digital maturity due to their widespread use and high degree of cross-border relevance, while, in Member States with higher numbers of cross-border workers, the incentives to digitalise coordination and request procedures are greater.

Importantly, digitalisation in the field of social security coordination offers several benefits. For instance, it allows for improved communication among social security authorities and between authorities and citizens. In addition, it facilitates the implementation of agreements among Member States for regular bulk exchanges of data relevant to social security coordination (e.g., notably, the exchange of death certificates for pension coordination). Thus, digitalisation both enhances the accessibility and efficiency of social security systems for mobile citizens and improves the accuracy of case processing in accordance with EU coordination rules ([2]).

Streamlined digital processes in cross-border social security coordination are beneficial for citizens, employers and institutions alike. Mobile citizens enjoy faster, more transparent access to their social security entitlements. Employers benefit from simplified administrative procedures and better facilitated cross-border employment. Social security institutions achieve greater operational efficiency, improved case-handling accuracy, and enhanced capacity for cross-border collaboration and fraud prevention. Streamlined digital processes in cross-border social coordination help to enable

---

([1]) Throughout this report, the term 'Member State(s)' is used to refer to these countries.

([2]) Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems (OJ L 166, 30.4.2004, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02004R0883-20190731) and Regulation (EC) No 987/2009 of the European Parliament and of the Council of 16 September 2009 laying down the procedure for implementing Regulation (EC) No 883/2004 on the coordination of social security systems (OJ L 284, 30.10.2009, p. 1, https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009R0987).

citizens to exercise their right to free movement and promote social inclusion, ultimately supporting the EU's vision of an integrated and fair labour market.

A key contribution of this report is its extensive analysis of digital maturity in social security institutions, including the benefits, challenges and resource needs. While digitalisation enhances operational efficiency, accuracy and cross-border collaboration, many institutions still face resource challenges. These include shortages in information technology skills and in regulatory knowledge among current employees, as well as funding constraints, especially when new technologies are perceived as having high implementation costs relative to low cross-border case volumes. The severity and nature of these constraints vary across Member States.

Four key priority areas for improvement have been identified that align with the digital maturity assessment framework: (i) enhancing the interoperability of Member States' databases (particularly for domains outside of the EESSI system), (ii) improving user accessibility and efficiency through digital tools, (iii) increasing process automation through robotisation and (iv) ensuring a high level of data security. To address resource limitations and enhance digital maturity, social security authorities have proposed several approaches, including increased outsourcing, staff training, fostering interinstitutional knowledge exchange and leveraging EU funding. These considerations and priorities from social security bodies across the EU are crucial for achieving a harmonised digital transformation of the sector in the most efficient manner.

1. Introduction

Regulations (EC) No 883/2004 and No 987/2009 on the coordination of social security systems set out the need for frequent communication between social security institutions from different EU Member States, and between institutions and their clients (e.g. claimants for benefits, recipients of benefits and employers / self-employed people). As technology and digital infrastructure evolve, communication and information exchange are increasingly shifting to an electronic format and digital services play a growing role in the functioning of social security schemes, including in cross-border exchanges.

Several initiatives have been adopted by the EU in recent years to facilitate, integrate and harmonise the digitalisation of public services, making efficient digital public services accessible to all EU citizens, including when they move between Member States. For instance, in 2018, the European Commission adopted the single digital gateway regulation (SDGR) ([3]), which develops a network of national online portals to provide EU citizens and businesses with information on how EU rules are applied in each Member State for cross-border users and how to access these pertinent administrative procedures online. Similarly, the EU electronic identification and trust services (eIDAS) regulation ([4]) facilitates secure cross-border transactions by establishing a framework for digital identity and authentication. To promote seamless digital services across the EU, the eIDAS regulation provides for the interoperability of national electronic identification (eID) schemes among Member States by establishing mutual recognition for eIDs issued by EU countries.

As social security remains under the jurisdiction of the Member States, coordinated by the EU, national authorities are largely responsible for ensuring that mobile citizens have access to social security. Digital services and tools help make it easier for EU mobile citizens, businesses operating across borders and Member States' administrations to deal with cross-border social security. They reduce the amount of paperwork and speed up the handling of claims by the institutions in charge, making cross-border interactions smoother. Digital services also can help to avoid errors (e.g. in applications) and can help social security institutions detect erroneous and fraudulent cases. The implementation of such digital solutions varies across Member States in terms of their availability, accessibility, scope and quality.

The mandate of the European Labour Authority (ELA) is to support the Member States and the European Commission to ensure that EU rules on labour mobility and social security coordination are enforced in a fair, simple and effective way. This includes activities relating to the digitalisation of cross-border cooperation between Member States in the area of social security.

In September 2023, the European Commission published its communication on digitalisation in social security coordination ([5]), in which it announced a study on further developments in the longer term in the digitalisation of social security coordination. The present ELA report aims to contribute to this study through a mapping and an assessment of the digital maturity of the tools and services developed by Member States for ensuring cross-border social security coverage to EU citizens.

This study's key objective is to assess the digital maturity of social security services in cross-border contexts in Member States. This is done by an evaluation of the digital services that each country offers. The services covered relate to the following branches of social security:

- sickness benefits in kind,
- sickness benefits in cash,
- maternity/paternity benefits,
- family benefits,
- unemployment benefits,

([3]) Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (OJ L 295, 21.11.2018, p. 1, https://eur-lex.europa.eu/eli/reg/2018/1724/oj).

([4]) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (OJ L 257, 28.8.2014, p. 73, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014R0910-20241018); Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European digital identity framework (OJ L, 2024/1183, 30.4.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183).

([5]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on digitalisation in social security coordination: facilitating free movement in the Single Market, COM(2023) 501 final of 6 September 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A501%3AFIN.

- pensions,
- accidents at work and occupational diseases (AWOD).

Digital tools and services will include those directly implementing the relevant obligations laid out in Regulations (EC) No 883/2004 and No 987/2009, as well as tools designed to support the determination of applicable legislation under Title II of Regulation (EC) No 883/2004 at the national level. Since the study focuses on cross-border contexts, purely national situations are not covered. However, it is important to note that several of the listed systems will also be used in situations without a cross-border dimension. The study's scope does not include the implementation of the electronic exchange of social security information (EESSI), which is a decentralised, closed system, overseen by the Administrative Commission for the coordination of social security systems and its Technical Commission for Data Processing, both composed of representatives of the Member States and the European Commission.

The study assesses the accessibility of the digital services of each Member State for citizens from another Member State and the suitability for cooperation between Member State authorities in a cross-border context. These include:

- online tools for application and/or digital delivery of portable documents (PDs) ([6]);
- national portals for the verification of the validity and authenticity of PDs (i.e. PD A1 and the European health insurance card (EHIC));
- national portals and online forms for claiming social security benefits and/or for reporting relevant changes in the personal circumstances for individuals residing or staying abroad;
- automated processes for granting social security benefits or the digital/online provision of life certificates.

1.1. Tools for cross-border cooperation of social security institutions: portable documents

When citizens from Member States exercise their right to free movement, they will in certain situations need a document that confirms their social security rights and obligations. Such confirmation is needed for applicable legislation, in order to determine the Member State in which social security legislation applies as well as to avoid paying contributions in more than one country. Furthermore, it is needed for access to healthcare (sickness benefits in kind), for access to unemployment benefits and as confirmation of entitlements to a pension benefit.

Under the previous regulations, Regulations (EEC) No 1408/71 and No 574/72, cross-border citizens received a copy of the e-form as documentation. For sickness benefits to people on temporary stay in other countries (including tourists), the e-form E111 was replaced by a plastic card, the EHIC, from 2004 ([7]). When Regulations (EC) No 883/2004 and No 987/2009 entered into force in 2010, the exchange of information was to be electronic, not on paper. Thus, it was no longer possible to issue a copy of the e-form to citizens, and instead confirmation of rights and obligations was given by PDs.

There are 10 PDs, including the EHIC. All of the PDs have a uniform layout and content structure so that they are easily recognised by all social security institutions in the EU. Table 1 illustrates the PDs, organised by social security domains ([8]).

([6]) European Commission: Directorate-General for Employment, Social Affairs and Inclusion, 'FAQ social security – claims and forms', n.d., https://ec.europa.eu/social/main.jsp?catId=857&langId=en&intPageId=980.

([7]) The EHIC was gradually phased in and became the sole valid documentation from 1 January 2006.

([8]) European Union: Your Europe, 'Standard forms for social security rights', European Commission website, https://europa.eu/youreurope/citizens/work/social-security-and-benefits/social-security-forms/index_en.htm.

Table 1. PDs under Regulation (EC) No 883/2004

Social security branch	Document	Purpose	Relevant articles of Regulation (EC) No 883/2004	Relevant articles of Regulation (EC) No 987/2009	Issuing authority and use
Applicable legislation	A1	Certifies that an EU or EFTA resident is subject to the social security legislation of another Member State	Articles 11–16	Article 19	Issued by the social security institution of the country where the citizen is insured
Healthcare benefits	S1	Certifies the entitlement to healthcare if an EU or EFTA resident does not live in the country where they are insured	Article 17	Article 24	Issued by the citizen's health insurance authority. Submitted to any health insurance authority in the country of residence
	S2	Entitles the holder to obtain planned medical treatment in another EU or EFTA country	Article 20	Article 26	Issued by the citizen's health insurance authority. Submitted to the health insurance authority in the country of treatment
	S3	Certifies the entitlement to healthcare in the former country of employment, generally provided to retired cross-border workers	Article 28	Article 29	Issued by the citizen's health insurance authority. Submitted to the health insurance authority of the country of former employment
	EHIC	Allows the holder to receive necessary medical treatment during temporary stays in the EU and EFTA countries under the same conditions and at the same cost as people insured in that country	Article 19	Article 25	Issued by the health insurance institution where the citizen is insured
Unemployment benefits	U1	Provides a statement of insurance periods to be considered in calculating unemployment benefits	Article 61	Article 54	Issued by the public employment service or the competent social security institution in the last country or countries of employment. Submitted to the national employment service in the country where unemployment benefits will be received
	U2	Authorises an unemployed person to continue receiving unemployment benefits while seeking employment in another country	Article 64	Article 55	Issued by the public employment service or the competent social security institution in the country where the citizen became unemployed. Submitted to the national employment service in the country where employment is sought
	U3	Provides information on changes in the situation of a person receiving unemployment benefits in another EU country, which might affect the person's entitlement to the benefits	Article 65	Article 56	Issued by the public employment service or the competent social security institution of the country where employment is sought, on the basis of a U2 form

Social security branch	Document	Purpose	Relevant articles of Regulation (EC) No 883/2004	Relevant articles of Regulation (EC) No 987/2009	Issuing authority and use
AWOD	DA1	Entitles the holder to healthcare in the case of work-related injuries while working in a different country from the one of insurance	Article 36	Article 33	Issued by the citizen's health insurance authority. Submitted to the health insurance authority of the country of work
Pensions	P1	Provides a summary of pension decisions taken by the different institutions in the EU countries where the person has claimed an old-age pension, survivors' pension or invalidity pension	Articles 50	Article 48	Issued by the pension authority to which a pension claim is made, once the authority has received details of the decisions made by the various authorities that have dealt with the claim

NB: EFTA, European Free Trade Association.

1.2. EU digitalisation initiatives: an overview

The first attempts to digitalise social security coordination in the EU (e.g. the telematics in social security (TESS) programme ([9]) were primarily aimed at making the coordination of pension benefits more efficient through the exchange of bulk information, for instance on personal identification numbers and confirmation of deaths between institutions. Unlike EESSI, the use of the TESS solutions was not mandatory, so the exchange happened between some, but not all, Member States.

As shown in this report, some of these solutions, especially on the exchange of death data and life certificates, are still in use. It should be noted that none of the TESS solutions had a user interface that could be utilised in services directed at individual cross-border citizens. For this reason, these solutions could not be extended outside the use by competent authorities.

Several initiatives to reinforce and support user accessibility to digital public services have been implemented in recent years, including the development of EESSI, mentioned above. Most other EU initiatives do not exclusively regulate access to social security services in cross-border situations, but provide an integrated approach to multiple public services, including access to social security.

The European social security pass (ESSPASS) pilot project ([10]) is designed to make it easier for individuals to exercise their social security rights when they are in another Member State. ESSPASS should enable various entitlement documents, such as the EHIC and PD A1 to be stored in an 'electronic wallet' (the European Digital Identity wallets) by cross-border citizens and shared/shown for verification purposes in other Member States.

Regulation (EU) No 910/2014, also known as the eIDAS regulation, establishes mutual recognition of eIDs offered by EU countries, provided that they meet certain regulatory requirements and have been notified to the European Commission ([11]). The eIDAS regulation aims to improve cross-border workers' access to certain digital services offered by other Member States by ensuring that they can securely authenticate their identities using a variety of documents in an electronic format. Several Member States already grant mobile EU citizens access to their digital government portals in line with the eIDAS regulation (see Section 3.1.1).

([9]) European Commission, 'TESS – Telematics in social security', European Commission website, 27 September 1996, https://cordis.europa.eu/article/id/7014-tess-telematics-in-social-security.

([10]) European Commission, 'European social security pass', European Commission website, https://ec.europa.eu/social/main.jsp?catId=1545&langId=en.

([11]) European Commission, 'eIDAS regulation', European Commission website, 4 April 2024, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation; Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European digital identity framework (OJ L, 2024/1183, 30.4.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183).

The single digital gateway regulation was adopted in 2018 ([12]) with a view to ensuring that online procedures were accessible to cross-border users in a non-discriminatory way. Through the single digital gateway, the EU provides infrastructure for the implementation of the 'once-only' principle through the establishment of the single online contact point, Your Europe ([13]). Through the Your Europe portal, mobile EU citizens can obtain information on their basic rights under EU law and access a network of national portals providing information on how EU rules are applied in each EU country for cross-border users. This includes information on social security rights and obligations. The SDGR mandates that each Member State must provide for the electronic submission of requests for certain administrative documents and receive the output electronically. These include, notably:

- requests to determine which social security legislation covers the holder (the output of which is PD A1);
- notifications of changes in the personal or professional circumstances of the person receiving social security benefits;
- applications for the EHIC;
- claims for pension and pre-retirement benefits from compulsory schemes;
- requests for data on pensions from compulsory schemes.

Moreover, the once-only technical system ([14]) is being developed to enable EU public authorities to securely exchange official documents and data as part of cross-border administrative procedures, in compliance with the SDGR. This system will mean that citizens and businesses are no longer required to submit certain supporting documents ([15]) alongside their applications or claims, facilitating their transition to work, live or retire when relocating within the EU. Its decentralised architecture links public authorities, allowing them to exchange evidence at the request of individuals or businesses ([16]).

In parallel with implementing these EU initiatives, Member States have adopted national initiatives to provide and enhance digital access to social security services to mobile EU citizens. This can be, for instance, through online portals, websites or apps where information can be consulted, requested, updated or received.

Differences in the organisation of social security institutions are one of the challenges in the digitalisation of social security coordination. Some countries, for instance the Nordic countries, have large 'one-stop-shop' institutions that cover most branches of social security (although no country has one institution that covers absolutely everything). Other countries, notably some of the largest (Germany and France), have separate organisations for each branch. Additionally, although social security organisations are typically organised at the national level, sometimes they can also be at the regional or the local level. Some countries, such as Denmark, divide the responsibility for social security between local municipalities for some benefits and highly centralised institutions for other benefits. Some countries (Germany, Austria and others) are federal states, where the responsibility for social security is divided between the state and federal levels. In other words, the organisational picture across the EU is quite complex. This is perhaps best illustrated by the fact that, in 2024, more than 3 400 different institutions across the EU were connected through the EESSI network.

It is not possible to address the full impact of organisational complexity in this report. It is, however, worth mentioning that many institutions are rather small, with limited information technology (IT) resources and limited capabilities for digitalisation in general. This may have an impact on the ability to provide digital solutions directed at cross-border citizens.

This report will present and discuss such initiatives in greater detail, in addition to measuring the digital maturity of such cross-border services in the Member States. The purpose of the report is to measure the implementation of such digitalisation efforts, in a number of core dimensions of digital maturity, and to provide an overall assessment of their digital maturity. These will cover user accessibility, but also data administration and exchange, interoperability and fraud/error detection. The report will map available resources and resource needs to further support the digitalisation of cross-border social security access at the national level across the Member States.

([12]) Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 (OJ L 295, 21.11.2018, p. 1, https://eur-lex.europa.eu/eli/reg/2018/1724/oj).

([13]) Your Europe offers information in all official EU languages (except Irish). It allows site users to filter information based on their profile (citizen/consumer or business) and Member State of interest. See the Your Europe website at https://europa.eu/youreurope/index.htm.

([14]) European Commission, 'Once-only technical system', https://ec.europa.eu/digital-building-blocks/sites/display/OOTS/.

([15]) The once-only technical system will facilitate the exchange of documents that are available in digital format. Thus, some supporting documentation alongside their applications may still be required from citizens.

([16]) European Commission, 'Interoperable Europe Act enters into force today', European Commission website, 11 April 2024, https://commission.europa.eu/news/interoperable-europe-act-enters-force-today-2024-04-11_en.

2. Methodology

2.1. Development of a digital maturity assessment framework

For the purpose of this study, a digital maturity assessment (DMA) framework was developed to measure the **functionality of digital cross-border social security coordination services** and how effectively they support and facilitate the application of EU rules on social security coordination. The framework was developed through extensive desk research of existing methodologies, the project expertise of team members and a collaborative workshop.

The study's scope and methodology were shaped by several key constraints, including a limited project timeline and the data collection methods, which allowed a maximum of six interviews per Member State and excluded user surveys. Moreover, there is no precise or rigid definition of digital maturity (Box 1). Therefore, several established models served as a foundational reference for this framework.

Box 1. Defining digital maturity

There is no clear and univocal definition of digital maturity or one framework for carrying out a DMA. Magnusson and Nilson (2020) define digital maturity as any model aiming to **measure the ability of an organisation to ascertain the benefits from digitalisation (**[17]), hinting at the fact that the concept of digital maturity is multifaceted and that a unique definition is lacking.

A DMA is therefore a structured approach to evaluating the state of an organisation's **digital capabilities, processes and practices**.

Several DMA frameworks have been developed in recent years by public and private organisations. Such digital maturity frameworks typically measure various dimensions, often broadly organised around the following: information and communications technology infrastructure, digital strategy, digital culture, customer or user experience, operational processes, data and innovation.

In recent years, specific DMAs have been developed for measuring the digital maturity of public sector organisations. The Organisation for Economic Co-operation and Development (OECD) has developed a digital government policy framework and index ([18]), whereas the EU has developed a DMA framework for public sector organisations through the European Digital Innovation Hubs network ([19]). The United Kingdom has developed a detailed digital functional standard for implementation across its public sector organisations ([20]). Academic models have also been developed in recent years to measure the digital maturity of public sector organisations, to a varying extent of detail.

The study is set against the complex backdrop of EU social security coordination; while Member States retain responsibility for organising national social security systems, the EU regulates coordination between these systems. The research aimed to assess the uneven development of IT services across Member States, comparing the implementation of digital tools and services for situations specific to cross-border social security coordination.

While a two-tier approach to assessing digital maturity – which includes both organisational-level maturity (as per the Swedish Center for Digital Innovation framework) and the functionality of cross-border social security coordination services – may provide a more comprehensive evaluation, this study focused primarily on the functionality aspect. Specifically, the DMA framework in this study emphasises how effectively cross-border social security services support and facilitate the application of EU rules. The DMA framework is centred on five main dimensions, as outlined in Table 2.

([17]) Magnusson, J. and Nilsson, A., *Digital Maturity in the Public Sector – Design and evaluation of a new model*, SWEG 2020, Gothenburg Sweden, https://gup.ub.gu.se/file/208009.

([18]) OECD, 'The OECD digital government policy framework: Six dimensions of a digital government', *OECD Public Governance Policy Papers*, No 02, 2020, OECD Publishing, Paris, https://doi.org/10.1787/f64fed2a-en.

([19]) European Commission, 'European Digital Innovation Hubs Network', European Commission website, https://european-digital-innovation-hubs.ec.europa.eu/home.

([20]) UK government, 'Standard: Digital and data continuous improvement assessment framework', GOV.UK website, 15 July 2024, https://www.gov.uk/government/publications/government-functional-standard-govs-005-digital/digital-and-data-continuous-improvement-assesment-framework-hmtl.

Table 2. Dimensions and subdimensions of the DMA framework

Dimension	Subdimension(s)	Description
Digital service accessibility	Online access for mobile citizens	The existence of centralised online portals for citizens to gather relevant information and initiate the application for benefits / PD request process
	Issuing digital documents	Whether citizens can receive digital versions of PDs
	Multilingual services	The availability and effectiveness of automated translations, multilingual chatbots and other tools that facilitate communication with clients in their native languages
Digital administration	Digital documents	The extent to which documentation is received and stored by authorities in a digital format for processing benefit claims or PD requests
	Automated processing	The extent and effectiveness of automation in the coordination and allocation of social security benefits in cross-border scenarios, as well as of automation of their recovery
	Digital communication	The extent to which institutions favour, encourage and implement digital communication channels with clients
Systems interoperability	Interoperable databases	The capability of systems to communicate across borders, including compatibility with systems in other Member States
	Agreements for bulk data exchange	The existence of agreements with other Member States for bulk exchange of relevant data for social security coordination
Network security and data protection	Tools for digital system security	Security protocols and compliance with EU data-protection laws to safeguard personal information during administrative procedures
	Secure communication	Strategies to ensure the protection of personal information during cross-border exchanges
Fraud and error detection	Digital tools/strategies for preventing error and fraud	The use and effectiveness of digital tools for fraud identification and error prevention

The DMA framework covers the functionality of existing instruments for social security coordination, including digital tools and services developed by the Member States, and how they contribute to ensuring the effective application of EU social security coordination rules, in particular the requirements set out in Regulations (EC) No 883/2004 and No 987/2009.

The DMA focuses on tools that help applicants to identify the social security scheme that applies to them, tools that facilitate information exchange between social security institutions (e.g. to detect cases of social security fraud or calculate due benefits) and digital services that facilitate the processes of requesting and granting benefits for each social security branch.

Each of the dimensions of digital maturity was matched with indicators to classify the digital maturity of Member States' digital social security services and coordination tools. Table 3 summarises the approach to objectively scoring each dimension.

Table 3. Scoring approach

Dimension	Indicators	Low maturity	Partial maturity	Full maturity
Digital service accessibility	Submit online requests for obtaining PDs or claims for social security benefits	No digital service	Online submission, but PDF forms	Online application forms
	Consult and update personal information online	No	—	Yes
	Receive digital versions of PDs	No	—	Yes
	Multilingual services	Only national languages	Limited multilingual options	Broad multilingual options
	Possibility to authenticate identity using foreign (secure) credentials	No	—	Yes
	Paper applications accepted and client support services available	No to both	Yes to one	Yes to both
Digital administration	Digitalisation of documents and implementation of DDMSs	No digital documents	Digitalised documents but no DDMS	DDMS
	Process automation for data verification (back-end checks with registries and translations)	No	Yes – manual verification	Yes – automatic verification
	Process automation for recovery of outstanding contributions and unduly paid benefits	No	—	Yes
	Process automation for requests for PDs and granting of benefits	No	—	Yes (human approval still needed)
	Digital communication with clients	No	Yes, but not secure	Yes, secure only
Systems interoperability	Databases interconnected with those of other Member States	No	—	Yes
	Databases interconnected at the national level	No	—	Yes
	Participation in bulk exchanges with other Member States (data agreements)	No	—	Yes
Network security and data protection	Measures in place for network security	No	—	Yes
	Measures in place for the protection of personal data (as per the general data-protection regulation)	No	—	Yes
	Secure communication channels (outside EESSI)	No	Yes, with clients only	Yes, with clients and cross-border partners
Error and fraud detection	Digital tools in place for detection of errors	No	Passive	Active
	Digital tools in place for detection of fraud	No	Passive	Active

NB: DDMS, digital document management system.

2.2. Data collection activities

The data collection approach consisted of two main assignments, aimed at gathering information needed for the analytical tasks. First, an inventory of the digital tools and services for cross-border social security coordination used in Member States was compiled. Second, semi-structured interviews were conducted with representatives of national social security institutions, representing the branches of social security covered by the study, on digitalisation initiatives for cross-border cases.

This study's DMA is based on the inventory, interviews with social security institutions in the Member States and supplementary EU-based desk research.

2.2.1. Inventory of digital tools and services for EU cross-border social security coordination

The information gathered to populate the inventory on cross-border services in the field of social security coordination was drawn from the following sources:

- the EU survey on PDs ([21]);
- an online search for information by the 30 country experts;
- the country factsheets of the European Commission's Access to Base Registries ([22]);
- information on the digital provision of EHIC replacement certificates ([23]) across countries gathered by the project team.

Information gathered through preliminary desk research using the abovementioned sources was validated as part of the interviews with representatives of national social security institutions. Additional information collected through interviews was incorporated into the final version of the inventory.

2.2.2. Interviews on implementation progress and the digital maturity assessment

Using the DMA framework developed for this study, a set of questions was drafted to form a data collection template to guide national experts' interviews with representatives of cross-border social security institutions, which was provided together with detailed instructions for the interviewers. The semi-structured interview guide was designed to facilitate comprehensive discussions, providing insights into the digital maturity of social security institutions from the perspectives of those managing and operating within them. It contained questions aimed at the mapping of digital tools and services used in the countries covered by the study in the inventory, at measuring the digital maturity of the cross-border social security services and at identifying potential obstacles to their implementation and/or deployment.

Target interviewees included:

- civil servants involved in the delivery of cross-border social security services in relation to the main social security branches covered by the study;
- civil servants involved in the development and implementation of the digitalisation strategy of the social security organisation and of cross-border services (e.g. working in IT);
- civil servants in leadership/management roles in the institutions responsible for the social security branches covered by the study;
- where experts from social security institutions were not available or able to provide comprehensive or complete answers, academic experts with specific expertise in the analysis or development of digital tools/services for cross-border social security services in the Member State concerned.

It is important to highlight that non-governmental stakeholders were not contacted within the context of this study (except when access to AWOD coverage was private), nor was a user survey carried out to gather primary data from users of social security services. The data collection effort focused on interviews with representatives of the social security institutions themselves and on developing a practical understanding of the digitalisation efforts implemented in this area. For a select number of countries, national liaison offices were consulted for support in identifying interviewees representing all social security branches covered by this study.

2.3. Methodological considerations

The field of digital tools and services for social security coordination is rapidly evolving (see Section 3.3). Many Member States are in the process of developing or implementing new digital initiatives. Where upcoming initiatives or those under development were identified (either through desk research or interviews), they were included in the present study. However, available information on these digital tools and services was less detailed, due to specific aspects still being under development or interviewees not yet having direct experience with such tools. As a result, the study may not fully capture the future landscape or the potential impact of these ongoing projects.

In countries where social security is not fully centralised within one institution, it was not always possible to speak with representatives of every social security branch. The scope of data collected by national experts therefore depends on the degree of social security centralisation in the Member States. Where coordination was very centralised, such as in Greece

([21]) European Commission, 2023. Results provided to the project team by the ELA.
([22]) https://interoperable-europe.ec.europa.eu/collection/access-base-registries/abr-member-states-factsheets.
([23]) Administrative Commission for the Coordination of Social Security Systems, Decision No S2 of 12 June 2009 concerning the technical specifications of the European Health Insurance Card (OJ C 106, 24.4.2010, p. 26, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2010_106_R_0026_01). This decision mandates that the EHIC card should be in the form of a physical, plastic card.

and Latvia, one group interview sufficed to gather the necessary data. Where several institutions deal with different branches of social security, experts had greater difficulties in covering all branches within the scope of the study due to difficulties in identifying relevant contacts or the availability of institutional representatives. This decentralisation led to some gaps in the data collection, as comprehensive insights from all relevant branches could not be obtained. An overview of how many interviews were conducted for each country, including the social security branches that were covered by interviewees, is presented in Annex B.

Similarly, identifying stakeholders with the necessary technical expertise to provide information covering all dimensions of the DMA framework posed some challenges. Owing to the organisational structure of social security institutions, identifying individuals who possessed both the technical knowledge of digital tools and the practical experience in their application was not always straightforward. The specialised nature of cross-border digital tools means that such expertise is often concentrated in a small number of individuals or, conversely, spread across various divisions responsible for the various steps of the process for receiving applications and granting benefits. It was not always possible to integrate the expertise and perspectives of all stakeholders for each social security branch in the report. However, the overall number of interviews carried out in the context of this report provides a comprehensive understanding of implementation progress across social security branches for the various dimensions of the DMA and the overall digital maturity of cross-border social security services in the Member States.

3. Results: progress in digitalising cross-border social security coordination

Key findings from this chapter

At the aggregate level, the digital maturity of cross-border services implemented by Member States can be summarised as follows:

- **User accessibility** is steadily progressing, with many social security authorities offering some form of online application platforms for requesting benefits and PDs. Supporting multilingual services and facilitating secure cross-border authentication for users are key areas for improvement to achieve full maturity in this dimension. The full implementation of the eIDAS regulation, which is predicted to take place by 2026, is expected to significantly contribute to the EU-wide integration of identity authentication systems.
- **Digital administration** is advancing in many Member States. Digital document handling is increasing as online platforms for benefit requests are increasingly utilised. Several social security institutions have also introduced automated processing in the benefit or PD approval process. Cross-border cases, however, still typically require human intervention due to their high level of complexity, which automation tools are often unable to resolve.
- **Systems interoperability** is the least advanced DMA dimension. The reason is twofold: first, EESSI is the interoperable system used for cross-border social security coordination. Cross-border interoperability of social security schemes outside this system is limited. Second, a range of practical challenges (e.g. data-protection concerns, constraints in data models and content/methodology, and administrative differences) render cross-border integration of databases particularly complex.
- **Network security and data protection** is the most advanced DMA dimension. This is linked to strong EU regulation in the field, notably the general data protection regulation. Several practical challenges of advancing digitalisation for cross-border social security coordination are linked to ensuring a high level of protection of sensitive data, in compliance with both EU and national legislation.
- **Error and fraud detection** is undergoing a digital transformation, with a few Member States making use of algorithms to identify errors and flag potential cases of social security fraud.

EU initiatives – such as the implementation of EESSI, the SDGR and the eIDAS regulation – have been **key driving forces** in securing a **minimum level of digitalisation** across Member States' social security services. In parallel, several Member States have implemented digital tools and services that complement EESSI with **national-level solutions** addressing specific cross-border coordination needs.

Member States vary significantly in their adoption of digital tools and services tailored specifically to facilitating cross-border social security coordination. The digital maturity of these initiatives differs across both Member States and social security branches. The most common forms of Member States' digitalisation initiatives, relevant for ensuring proper implementation and uptake of cross-border social security benefits, are:

- **online and remotely accessible portals** for requesting PDs or applying social security benefits;
- promoting **secure digital communication** between social security institutions and clients;
- signing agreements with other Member States for **regular bulk exchanges of data**;
- developing **digital tools for error and fraud detection** in the field of social security.

Several Member States have implemented (or are currently developing) novel digital tools and systems, paving the way towards **innovative and effective solutions** to improve the field of cross-border social security. Key initiatives, which can be considered **good practices** to be encouraged across the EU to foster effective cross-border coordination, include:

- prefilling applications with data retrieval from registries and automated eligibility verification through data matching;
- automatic generation and digital emission of PDs;
- complementary mobile applications for users to initiate administrative procedures and securely communicate with social security institutions;
- online tools for third-party authentication of PDs;
- setting up interoperable databases for field-specific data retrieval across borders.

The digital transformation of cross-border social security services through the implementation of digital tools to facilitate cross-border coordination of social security benefits represents a crucial step in ensuring seamless access to social protection for mobile EU citizens. In particular, digitalisation efforts help to streamline processes to ensure easy access to and efficient execution of various essential services for cross-border workers. These include applications for PDs, benefit claims, updating personal information and communication with social security institutions across Member States. As more Member State citizens exercise their right to live and work in different EU countries, the need for efficient, accessible and interoperable digital services becomes increasingly apparent.

Digital tools and services also play a vital role in enabling social security authorities to coordinate and exchange cross-border data, thereby facilitating their communication. This aspect is particularly crucial in cross-border cases compared with national cases, as such tools and services allow complex scenarios involving multiple Member States to be handled more efficiently and efficient tackling of cross-border social security fraud.

This chapter is structured according to the dimensions of the DMA framework developed as part of this study. It is therefore categorised according to the five dimensions of digital maturity identified:

1. **digital service accessibility**, which evaluates the functionality and user-friendliness of online tools for applications and the digital delivery of PDs, as well as the availability of multilingual services;
2. **digital administration**, focusing on the extent of automated processing in benefit allocation and the implementation of digital communication channels with clients;
3. **systems interoperability**, assessing the interoperability of authorities' systems and databases, as well as bulk data exchanges between Member States;
4. **network security and data protection**, assessing the robustness of security protocols for personal data protection;
5. **error and fraud detection**, examining the use and effectiveness of digital tools for identifying fraud and preventing errors in cross-border social security processes.

It aims to provide a deeper and more comprehensive evaluation of the current state of digital service provision in cross-border social security coordination and to identify the main barriers to and areas for further development and harmonisation across the EU. This analysis will encompass both the citizen-facing aspects of digital services and the crucial interinstitutional communication and data-exchange processes that underpin effective cross-border social security coordination.

Thus, this analysis complements the inventory of digital tools and services that accompanies this report by providing a qualitative evaluation of the main trends that can be identified with regard to the status of digitalisation across the social security branches within the scope of this study. Furthermore, this section presents some of the best practices identified by social security authorities across the EU to highlight how digitalisation can be best integrated into social security coordination processes.

3.1. Digital service accessibility

Key findings from this section: digital service accessibility across Member States

Digital maturity in this dimension across the Member States can overall be considered**:**

PARTIAL

Almost every Member State has established online portals for digital requests of A1 PDs and EHICs, in line with SDGR requirements. However, there is a marked disparity between these portals' digital sophistication and accessibility, as well as significant variance in Member States' implementation of similar online portals for claiming benefits and requesting PDs for other branches of social security.

The most common types of portals offer basic online information and partially digitalised processes, often requiring PDF downloads for application forms and postal correspondence, alongside authentication systems restricted to national credentials. In contrast, more advanced systems – such as those found in Finland, Norway and Slovenia – provide comprehensive digital services with automated data prefilling, multilingual interfaces, digital document delivery and more inclusive authentication methods.

The main benefits of accessible digital services include boosting benefit uptake and more efficient cross-border employment processes through streamlined, user-friendly digital platforms. Allowing users to easily update their information online, for instance, also helps reduce error and minimise unduly paid benefits. A key aspect of digital maturity in this dimension is the importance of maintaining both digital support services (e.g. chatbots and helplines) and traditional communication channels to ensure inclusive access for all citizens, regardless of their digital literacy or access to information and communications technology.

Typically, there is no specific portal dedicated to cross-border users, meaning that all citizens must submit their claims through the same online access point. Consequently, the main obstacles that cross-border workers face are remotely accessing portals without national identification, limited language options and paper-based applications that require postal correspondence. These gaps can be addressed by the pending full implementation of the eIDAS regulation for secure cross-border authentication, the ongoing transition from paper to digital documents and the development of multilingual digital services across national social security institutions.

The EU single market project places a strong emphasis on service accessibility, including in relation to digital cross-border social security. In fact, the **EU digital single market strategy**, launched in 2015, identifies better access to digital goods and services across Europe as one of its three key pillars ([24]). The importance of user accessibility in the digitalisation of public services was reinforced in the 2021 European Commission communication on the 2030 digital compass, in which one of the key objectives to be achieved by 2030 was to ensure that citizens can easily make full use of online services in the public sector throughout the EU, while preserving privacy ([25]). Digital access to cross-border social security services is a key part of such access to public services for EU citizens, when exercising their right to free movement across the EU.

Regulatory efforts aim to ensure that EU citizens in cross-border situations can easily access social security services, upholding the principle of equal treatment and non-discrimination, which ensures that EU citizens have the same rights and obligations as nationals of the country where they are covered ([26]). The initiatives that have aimed to improve accessibility include the online provision of information in multiple languages, the implementation of digital tools and services to facilitate applications for benefits and the issuance of documents, reducing paperwork and red tape, and expediting the administrative processes involved in granting access to social security coverage to mobile EU citizens. EU legislation provides a framework for ensuring digital access to social security services ([27]).

3.1.1. Online access to cross-border social security benefits for mobile citizens

Regulation (EC) No 883/2004 establishes the principle of equal treatment in cross-border social security situations, entitling EU mobile citizens to claim social security benefits in cross-border situations. These include claims for:

- **pension benefits** accrued in another EU country from a certain period of time;
- **sickness or family benefits** from workers residing in one EU country while being insured in another one, such as frontier workers;
- **AWOD benefits** from a worker that has suffered a work-related injury in a different country from the one of insurance.

However, Regulation (EC) No 883/2004 does not provide for common social security schemes at the EU level. Instead, the regulation coordinates national social security schemes via statutory rules on applicable legislation. These rules, in turn, determine which national scheme every EU citizen, including cross-border individuals, belongs to.

([24]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A digital single market strategy for Europe, COM(2015) 192 final of 6 May 2015, https://ec.europa.eu/commission/presscorner/api/files/attachment/8210/DSM_communication.pdf; and Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – EU eGovernment action plan 2016–2020 – Accelerating the digital transformation of government, COM(2016) 179 final of 19 April 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016DC0179.

([25]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 2030 digital compass: the European way for the digital decade, COM(2021) 118 final/2 of 9 March 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0118%2801%29&qid=1724950173447.

([26]) Article 4 of Regulation (EC) No 883/2004 mandates equal treatment for individuals covered by the regulation and nationals of the Member States. Equal treatment involves ensuring user accessibility for, for example, posted or EU mobile workers.

([27]) Key regulations include Directive (EU) 2016/2102 on the accessibility of the websites and mobile applications of public sector bodies, Directive (EU) 2019/882 on the accessibility requirements for products and services and the SDGR (Regulation (EU) 2018/1724).

One consequence of the coordination rules is that cross-border access to social security benefits may be **more complex** than purely domestic applications. For instance, the information may not be available in the native language of the applicant, they might need additional paperwork such as the presentation of further documentation (i.e. PDs, as Section 3.1.3 will illustrate) and they might require coordination with social security institutions from other Member States.

Digital and online procedures to claim benefits have the potential to reduce complexity and improve user accessibility to social security benefits for mobile EU citizens. In this context and in parallel with the digitalisation efforts at the EU level presented above, several Member States have implemented initiatives for digitalising social security application procedures in cross-border situations and for ensuring that mobile EU citizens have access to information on the requirements for exercising their social security rights.

In recent years, Member States have made **clear progress** in incorporating digital tools into their social security **application** and coordination processes, reflecting their commitment to improving accessibility and efficiency. These include the development of online systems for users to submit and manage their benefit application. The degree and nature of digitalisation of the benefit application process varies significantly across Member States, with some having fully digitalised systems and others still developing their digital services.

Digital submission of benefit applications or requests for portable documents

Online portals are the most common approach used by relevant bodies and institutions across social security branches to provide a centralised access point for citizens to gather relevant information and initiate the benefit application process ([28]). These portals are typically centralised to reflect the degree of centralisation of the organisational structure of social security coordination bodies at the national level. In other words, if multiple social security domains are coordinated by a single body, EU mobile citizens can apply for a benefit or request several types of documents through a single access portal online.

Overall, **all Member States reported the availability of at least one such online portal**, as presented in the accompanying inventory of digital tools and services (Annex A). However, the extent of digitalisation for the process of **applying** for social security benefits varies significantly across Member States, including **across social security branches** within the same country.

Progress in relation to user accessibility may be considered as one of three broad categories:

- continuing prevalence of paper-based applications;
- submission of downloadable digital forms (e.g. via email);
- fully digitalised request and submission procedures.

In some countries, traditional **paper-based applications** remain prevalent for certain benefit applications and requests for PDs. For instance, in the Netherlands, sickness benefits in kind require the submission of offline paper forms, even though, for other benefits in the same country, the process is highly digitalised. Similarly, Bulgaria and Luxembourg currently maintain only physical paper submissions for family benefits. In Norway, PD U1 and PD U2 are excluded from the online application process due to an outdated national IT system ([29]). In Cyprus, it is currently not possible to request PD A1, PD U1 or PD U2 online; however, the Ministry of Labour and Social Insurance is aiming to ensure that 80 % of procedures are carried out online once automated application procedures are implemented ([30]).

Notably, all countries still allow paper-based applications **alongside digital solutions**. This either may be because of legal obligations or practical requirements or may be a service for citizens to ensure inclusivity, in line with the European declaration on digital rights and principles for the digital decade ([31]). In the Netherlands, for instance, there is a legal obligation requiring public authorities to offer all digital services also in a paper-based form to reach citizens who are less familiar with digital processes and the online environment. Moreover, paper alternatives remain crucial insofar as electronic authentication remains an issue for cross-border workers to access digital services and solutions.

In contrast, several countries facilitate the **submission of digital forms** via email. More specifically, some institutions provide downloadable and electronically submissible versions of application forms for PDs or benefit claims, which are filled out and then returned either by email, often using e-signature, or via the authority's online portal. In Greece, cross-border users' application procedures mainly take place via traditional forms sent by email. In Luxembourg and Slovenia, unemployment benefits can currently be requested via email, either with physical signature of the document (Slovenia) or

([28]) See the inventory of digital tools and services accompanying this study (see Annex A) for more a complete mapping across Member States.
([29]) Interview with the national insurance administration of Norway (28 June 2024).
([30]) Interview with the Ministry of Labour and Social Insurance of Cyprus (9 July 2024).
([31]) European Commission, European declaration on digital rights and principles for the digital decade, Chapter II – Solidarity and inclusion (OJ C 23, 23.1.2023, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001).

with supporting documents (Luxembourg). For other benefits, Luxembourg has developed an online platform (MyGuichet) in which it intends to incorporate unemployment benefits at a later stage ([32]). Croatia and Slovenia are also relying on email for specific communications and submissions in the areas of pensions and health insurance while they develop their online service capabilities.

A growing number of Member States have embraced **fully digital solutions**, providing platforms on which forms can be completed and submitted online through institutional access portals, for some or nearly all social security branches. Key examples are shown in Box 2.

Box 2. Good practice: fully digital solutions for social security services using comprehensive online portals

Austria, **Belgium**, **Finland** and **Norway** manage most or all health insurance processes through online portals.

Germany's pension and unemployment benefit branches are largely automated, allowing the online submission of applications by cross-border users. Additionally, PD A1 is applied for via a payroll accounting programme or a completion aid on a national portal.

Finland offers a comprehensive online platform, OmaKela, across all branches of social security. More than 90 % of PD A1 applications are submitted electronically through the Finnish Centre for Pensions.

The availability across social security branches of online portals to apply for benefits and request PDs varies in Member States. On the one hand, **applications for pension benefits and A1 PDs are consistently digitalised**, in line with the obligations set out in Annex II to the SDGR. On the other hand, the digitalisation of benefit applications or PD requests for the remaining social security branches (unemployment, AWOD, sickness, family and maternity/paternity benefits) are left to Member States' discretion.

For branches of social security for which there are no digital requirements under the SDGR, digitalisation typically varies at the (national) institutional level. As a result, in countries with high levels of administrative centralisation, such as Finland, digital application services are available across several (if not all) social security branches. In countries with several social security institutions involved, digital applications may be less evenly available, also depending on the type of information required for the specific benefit being applied for. For instance, in Czechia, electronic interactive forms and/or online applications are available for all social security services in the area of pensions, sickness in cash and the determination of applicable legislation (PD A1). For most of these services, the Czech Social Security Administration (CSSA) offers two methods of completion: either without logging into the CSSA e-portal or with the automatic loading of data (which requires logging into the CSSA e-portal using either national or EU certificate). Most of the services are also available in English
For unemployment benefits, while U1 PDs can be requested online, the U2 document, which authorises the payment of unemployment benefits abroad, should be requested in person by the claimant. Family benefits can also be applied for through the Jenda portal ([33]) of the Ministry of Labour and Social Affairs. However, certain cases with a cross-border element may necessitate closer contact with the client. In such instances, the claimant may be required or offered to visit a branch office in person at least once, particularly if residing within Czechia or and online or phone consultation.

Digitalisation processes are being implemented progressively throughout the Member States, and **further initiatives** are in the pipeline in a number of countries. For instance, in Slovakia, digitalisation processes are being developed as part of the National Recovery and Resilience Plan. The national Social Insurance Agency aims to create pre-completed forms with information held by the agency's systems, so that users would be required to fill out only the data that the Social Insurance Agency does not already possess. In Luxembourg, there are plans to incorporate unemployment benefit applications into the online MyGuichet platform, as part of the ongoing digitalisation initiative.

Applications for mobile devices

Applications for mobile devices are available or currently under development in several Member States to complement social security online portals, thereby enhancing user accessibility. This is particularly evident in the health insurance branch, but also for pension benefits (Spain) and applicable legislation assessments (Belgium). Key examples are shown in Box 3.

([32]) Interview with the national employment agency.
([33]) See https://jenda.mpsv.cz/.

Box 3. Good practice: mobile applications for digital social security services

The **Austrian** MeineÖGK app allows users to declare if they have lost their EHIC and provide a service for issuing replacement certificates. The **Polish** MojeIKP app allows to check the validity of the issued EHIC, request for an EHIC or a replacement certificate.

In **France**, the Ameli app facilitates numerous procedures under the sickness and AWOD branches. The app allows certificates of entitlement to be downloaded, personal data to be managed, medical certificates for an accident at work or occupational illness to be sent to the competent fund, EHICs to be ordered and viewed, and even the registration of newborn children.

In **Poland**, applications for family benefits can be submitted directly via the mZUS app.

In **Luxembourg**, the MyGuichet platform (for management of family benefits, AWOD, sickness benefits and maternity/paternity benefits) has a mobile application allowing users to, inter alia, add attachments to active procedures directly from their smartphone or tablet, find messages exchanged with administrations and public bodies within the framework of online procedures directly, and track the status of active procedures.

In **Spain**, the Vivess app was recently launched for pensioners residing abroad to fulfil the annual procedure of accrediting that they are alive, allowing them to obtain immediate confirmation of their updated status. Without the application, a pensioner must go to the consulate or embassy to confirm proof of life in person. The Vivess app aims to minimise this bureaucratic procedure. The app recognises each person by biometric identification, asks them to smile to prove that they are alive and issues a certificate that can be signed digitally. The certificate is then automatically sent to the Spanish benefits database directly.

Belgium is developing initiatives to further facilitate the submission of relevant information through mobile devices. For instance, pilot projects have been set up by the Belgian national social security institution to introduce speech technology (e.g. Siri, Alexa or Google Assistant) for the submission of a work declaration in Dimona, the software used by the authorities for the immediate declaration of the start and end time of employment by employers ([34]). Such initiatives, relevant for all workers employed in Belgium, are expected to contribute to greater accuracy in employment declarations, which are relevant for determining the applicable social security legislation and in combating social security fraud.

Updating of personal information

Allowing mobile users to **update personal information in a timely manner** in the EU cross-border social security context is a crucial aspect of digital accessibility. First, it minimises the risk of **errors**, for instance in the payment of a benefit resulting from the failure to update new bank account information or the delivery of a PD (e.g. the EHIC) to an outdated home address if the applicant has moved since the request was submitted. Second, having correct information reduces the risk of **fraud or overpayment**, such as claiming residency in two countries to take advantage of multiple systems. Third, facilitating the updating of information through digital procedures improves **user friendliness and flexibility** and allows the necessary updates to be received and processed more rapidly. Ultimately, correctly updating information will facilitate national administrative processes and the exchange of information between social security institutions within the same countries and across Europe, with lower risks of contradicting information appearing in the data systems managed by various institutions.

In many Member States, social security bodies offer citizens the possibility of updating their personal information, reporting changes in their circumstances or reviewing the status of their claim **via online portal procedures** (Box 4 outlines an example of the automation of this process). However, there is significant room for more complete implementation of this feature, which does not appear to be systematically implemented.

([34]) RSZ, *De RSZ: Geld, gegevens en sociale zekerheid*, Brussels, 2020, https://news.belgium.be/sites/default/files/news-items/attachments/2020-02/dossierPresse_170220_nl_v4.pdf.

Box 4. Good practice: automated processes for updating personal information in Finland

In Finland, the process to update personal information is automated on the **online portal** of the Finnish Centre for Pensions. Changes in the circumstances of the employer or employee can be reported directly via the electronic application service.

The electronic application service reacts to the person's situation and **only asks the questions that are relevant for making the decision**, bringing data directly from registers (e.g. regarding the company and addresses of both the employee and the employer). Consequently, there is **no need to add attachments** to the application.

The A1 automation resolves applications in less than an hour and a posted worker's PD A1 is usually obtained by answering fewer than 10 questions.

The need to ensure that there is an accessible and facilitated process to allow cross-border users to update their personal information and report any changes to their circumstances is particularly useful for those national authorities that lack information about mobile citizens that it may hold for its own nationals. For example, the Central Administration Office (Centraal Administratie Kantoor (CAK)) in the Netherlands (responsible for sickness benefits in kind) ([35]) noted that, by the time it sends an S1 or EHIC in physical format, the recipient's address may have changed from a temporary address upon arrival to a secondary or more permanent address in the host country. CAK frequently becomes aware of delivery failures only when the documents are returned. In such cases, further enquiries must be made, for example with the Sociale Verzekeringsbank and pension insurers, to obtain the correct address, which can sometimes be challenging. Currently, there is no online system in place to update addresses.

This issue was further highlighted by the Belgian National Social Security Office ([36]) in the specific situation of seasonal workers, such as those from Poland and Romania, who are temporarily enrolled in the Belgian social security system and entitled to additional payments. Distributing these payments after the workers' return to their home countries presents difficulties due to unreliable contact information and scepticism towards electronic communication. In response, Belgium is exploring the implementation of an electronic wallet or e-box system to streamline communication and payment processes. However, overcoming logistical challenges and ensuring workers' trust and engagement with this new system are key to the success of this initiative.

Accessibility and inclusion

Digital social security services bring both opportunities and challenges for accessibility and inclusion. The EU has implemented two key directives to enhance the **accessibility and inclusion of digital services**. First, Directive (EU) 2019/882 on the accessibility requirements for products and services outlines specific accessibility requirements in Annex I. Second, the web accessibility directive (Directive (EU) 2016/2102) ([37]) requires an accessibility statement for each website and mobile app, a feedback mechanism for users to report accessibility issues, and regular monitoring and reporting by Member States. An evaluation in 2021 ([38]) found that all Member States had integrated the requirements of the web accessibility directive into national legislation and had begun activities to improve the accessibility of public sector websites and mobile applications.

While many Member States have made progress in this area, research indicates that there remains **significant room for improvement** to ensure that vulnerable groups are not left behind. Despite these efforts, issues persist that hamper progress in digitalisation. The most significant of these is the level of digital literacy among vulnerable groups, such as older people, which can result in high non-take-up rates of benefits or in additional costs for claimants who require paid assistance to access online application processes. For this reason, it is important for social security bodies to continue accepting traditional paper-based applications related to cross-border social security sources to ensure that no citizen is excluded from the provision of social security services. The availability of help centres for navigating digital procedures and the maintenance of non-digital communication channels are similarly crucial to providing accessible and inclusive public services.

([35]) Interview with CAK (8 July 2024).

([36]) Interview with the National Social Security Office (12 July 2024).

([37]) Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (OJ L 327, 2.12.2016, p. 1, https://eur-lex.europa.eu/eli/dir/2016/2102/oj/eng).

([38]) Commission staff working document evaluation – Review of the application of Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies (web accessibility directive), SWD(2022) 410 final of 7 December 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022SC0410.

According to a 2022 European Social Policy Network report ([39]), most online portals providing information on social protection are accessible to people with visual or hearing impairments. Nonetheless, it highlights that access to information for vulnerable people needs to be improved and, crucially, that there is a need for systematic and comprehensive assessment of accessibility for people with disabilities. Despite the trend towards digitalisation, maintaining physical offices remains crucial to ensuring that no one is left behind. Face-to-face contact is often essential, particularly for older people seeking to access healthcare benefits. To this end, the report recommends that training be provided on site for frontline staff to ensure that they can meet the needs of people with low digital literacy and those with disabilities.

3.1.2. Issuing digital documents

Several Member States offer the possibility of issuing **PDs in a digital format**, most typically in PDF format. This includes, most notably, **A1 PDs**, in line with SDGR requirements.

The degree of digital processing of PDs across the Member States is notably heterogeneous (Table 4). Certain countries such as Denmark and Liechtenstein demonstrate comprehensive digital capabilities across almost all PD categories, while others, such as Cyprus and Greece, show minimal to no digital implementation beyond SDGR requirements. This suggests that the digital transformation of PD processing is **not progressing uniformly across document type or Member States**.

([39]) Spasova, S., Atanasova, A., Sabato, S. and Moja, F. *Making access to social protection for workers and the self-employed more transparent through information and simplification – An analysis of policies in 35 countries*, Publications Office of the European Union, Luxembourg, 2023, https://data.europa.eu/doi/10.2767/017942.

Table 4. Digital requests and delivery of PDs in Member States

	EHIC		A1		P1		S1		S2		S3		DA1		U1		U2		U3	
	Online request	Electronic replacement certificate	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output
AT	Y	Y	Y	Y			Y	Y			Y	Y								
BE	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	Y	N	Y	Y	Y	Y	N	N
BG	Y	N	Y	N	N	N	Y	N	N	N	Y	N	Y	N	A	Y	Y	Y	Y	Y
CY	N	N	N	N									N	N	N	N	N	N	N	N
CZ	A	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N
DE	A	Y	Y	Y	A	Y	N	N	N	N	N	N	N	N	Y	N	N	N	N	N
DK	Y	Y	Y	Y	Y	Y	Y	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
EE	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y
EL	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
ES	Y	Y	Y	Y	N	N	Y	N	N	N	N	N	N	N	N	N	N	N	N	N
FI	Y	N	Y	Y	N	N	Y	N	Y	N	Y	N	Y	Y	Y	Y	Y	Y	N	N
FR	Y	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	Y	Y	N	N	N	N
HR	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
HU	Y	Y	Y	Y	N	N														
IE	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N
IS	Y	Y	Y	Y	Y		Y		N		N		Y	A	Y					
IT	N	N	Y	Y	A	Y	N	N	N	N	N	N	N	Y	N	N	N	N	N	N
LI	Y	Y	N	Y	N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
LT	Y	Y	Y	Y																
LU	A	Y	N	N	N	N	Y	N	Y	N	Y	N	A	N	Y	Y	Y	Y	N	N
LV	Y	N	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	N	Y	N	N	N
MT	N	N	Y	Y	N	N	N	N	N	N	N	N	N	N	Y	Y	Y	Y	N	N
NL	Y	N	Y	Y	A	N	Y	N	Y	N	Y	N	Y	N	Y	N	N	N	N	N
NO	Y	N	Y	Y	A	Y	Y	Y	Y	Y	N	Y	N	Y	Y	Y	Y	Y	N	N
PL	Y	Y [2]	Y	Y	Y	Y	N	N	N	N	N	N	N	N	Y	Y	Y	Y	Y	Y
PT	Y	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y
RO	Y [1]	Y																		
SI	Y	Y	Y	Y	N	N	N	N	N	N	N	N	N	N	Y	N	Y	N	Y	N

	EHIC		A1		P1		S1		S2		S3		DA1		U1		U2		U3	
	Online request	Electronic replacement certificate	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output	Online request	Electronic output
SE	Y	N	Y	Y	N	N	Y	N	Y	N	N	N	N	N	N	N	N	N	N	N
SK	Y	Y	Y	Y	N	N	Y	Y	N	N	N	N	N	N	N	N	N	N	N	N

([1]) Online requests are possible, but only with a Romanian Internet Protocol (IP) address.
([2]) When a provisional replacement certificate is requested.
NB: Y, yes; N, no; A, automatically issued to the citizen. Blank cells mark missing data.
Source: Milieu Consulting, based on the EU survey, interviews and desk research. Information for Hungary and Poland obtained through consultation with their delegations to the Technical Commission for Data Processing in January and February 2025.

The EHIC and PD A1 demonstrate the highest level of digital maturity in terms of user accessibility, with a clear majority of Member States offering online request facilities for these documents (in line with SDGR requirements). For instance, 24 of the 30 Member States provide an online process for EHIC requests (Box 5 describes good practices), of which 13 Member States also issue digital temporary replacement certificates for the EHIC. Digital PD A1 applications are enabled in 25 Member States, of which 24 issue PD A1 electronically.

Regarding the relationships between other social security branches, U1, U2 and S1 PDs show moderate levels of online availability. The least digitally accessible documents are S2, S3 and DA1 PDs, with only a handful of countries offering digital services for these.

Having the option to receive digital copies of relevant social security documentation is particularly practical for cross-border and mobile workers. This is best illustrated by the case of the Netherlands, where there is currently no digital service implemented for receiving sickness benefits (in kind) by CAK, which covers half of the people insured in the Netherlands and living abroad ([40]). As a result, the process for receiving S1 PDs is still paper based. Both PD S1 and the EHIC are dispatched by post, with PD S1 containing special watermarks for security. Difficulties have been reported when dealing with foreign addresses as mentioned above. Moreover, pensioners or workers relocating abroad may experience delays in receiving their S1 statement or EHIC because of delays in delivery by the postal services. While the health insurance process is mostly paper based in the Netherlands, this is not the case, for instance, for requesting unemployment benefits, a process that is highly digitalised in the Netherlands.

Box 5. Good practice: digital solutions for cross-border EHIC applications

In several Member States, national health insurance providers now offer the possibility of issuing a **digital version of a temporary replacement certificate for the EHIC**. The digital replacement certificate of the EHIC grants EU citizens temporary access to health insurance while awaiting the physical card.

This is currently possible in **Austria**, **Belgium**, **Denmark**, **France**, **Germany**, **Greece**, **Hungary**, **Iceland**, **Liechtenstein**, **Luxembourg**, **Poland**, **Romania**, **Slovenia** and **Spain**.

Importantly, an ongoing project to **digitalise the EHIC** is currently being undertaken by the Administrative Commission for the Coordination of Social Security Systems.

Several social security institutions across the EU also provide online verification tools for users abroad to **verify the validity of PDs, particularly A1 PDs** (see Section 3.5). This is, for instance, the case in Portugal (applicable legislation) and Croatia (pensions), where all electronic documents issued have a verification code or a specific QR code that allows users to verify authenticity via a link provided. In Slovenia, users can verify both received documents (digital or printed) and downloaded digital originals using the online document verification service of the Pension and Disability Insurance Institute of Slovenia (ZPIZ).

3.1.3. Language accessibility

Multilingual services play a pivotal role in ensuring cross-border workers' access to digital social security services. As the EU continues to promote labour mobility and integration, an increasing number of citizens find themselves working in Member States where they may not be fluent in the local language. This linguistic diversity presents a significant challenge for national social security systems, which must cater to a workforce with varied language backgrounds.

The provision of multilingual services is not merely a matter of convenience; it is essential for guaranteeing that cross-border workers can fully understand their rights, their obligations and the processes involved in accessing social security benefits. Without adequate language support, these workers may face barriers in navigating complex administrative procedures, potentially leading to misunderstandings, delays in benefit claims or even the unintentional forfeiture of entitlements. Therefore, the development and implementation of effective multilingual support services are crucial for fostering equal access to social protection, promoting social inclusion and ultimately supporting the EU's vision of a truly integrated labour market.

In the realm of digital social security services, the **provision of multilingual support services varies significantly across Member States**. Most countries offer at least some information in English alongside their national language(s) on their social security websites and digital platforms:

([40]) Interview with CAK (8 July 2024).

- Belgium, Czechia (Box 6), Lithuania and Austria stand out by providing services in multiple languages beyond English, including the languages of neighbouring countries and major immigrant communities. Denmark, Spain, France, Luxembourg, Slovakia, Finland and Sweden typically offer bilingual support, usually in the national language(s) and English.
- Other countries, such as Croatia, Greece, Hungary, Latvia, Malta, Portugal and Iceland, do not report any significant multilingual digital services.

Box 6. Good practice: multilingual social security services in Czechia

The CSSA has implemented a range of **multilingual services** and initiatives to cater to its diverse clientele. The e-portal, primarily available in Czech, offers certain services in English, particularly those related to applicable legislation (PD A1), pensions, insurance history information, changes in personal status and payments to Czech authorities.

The CSSA provides **extensive language support** through its **international website**, which includes **detailed information** on national legislation, procedures, forms and EU/international agreements in English, French, German, Russian and Ukrainian. The website features frequently asked questions, links to relevant EU websites and lists of foreign insurance institutions in both Czech and other relevant languages.

Notably, the CSSA also organises **international consultancy days**, during which cross-border aspects related to Germany, Austria and Slovakia are explained, and **interpretation services** are available for clients. Similarly, in Austria, the Pension Insurance Institute holds regular international consultation days for insured people who have also earned pension periods in Croatia, Czechia, Germany, Hungary, Italy, Liechtenstein, Serbia, Slovakia, Slovenia and Switzerland. Belgium has similar events featuring simultaneous interpretation in French and Dutch, open to a wide audience of employers, employees and any other interested organisations.

A key element that emerged from national research is that language accessibility concerns not only the variety of national languages in which given digital services are available, but also **the extent to which the chosen terminology is understandable** to the individuals completing the process.

For instance, in the case of Luxembourg, the current policy is not to offer support in all languages on future platforms, but instead to offer support only in the official languages of Luxembourg, which hinders the creation of an expanded multilingual service. The need to ensure language accessibility was underscored by Luxembourg's National Employment Agency, which noted that users (cross-border or not) often face difficulties because the application forms for benefits and U1 PDs are quite lengthy, technical and written in complex language, making them hard to understand, particularly for cross-border workers and those without a higher education. However, there are no plans to add new languages, as services have found that people who need a language option (e.g. Portuguese, the most common case) often do not have the proficiency to complete the very technical forms in their native language. Therefore, the priority in the upcoming system reform is to significantly simplify the language used. Similarly, the CSSA in Czechia notes that translators are partially employed for communication with users in their languages, as translation is particularly beneficial for direct client communication to ensure that clients comprehend the content effectively.

The implementation of advanced translation technologies appears rather varied across the EU. While **chatbots** are available in a few countries, including Spain, Luxembourg and Finland, they are often restricted to the national language(s). Box 7 discusses such chatbots.

Box 7. Advantages and disadvantages of multilingual chatbots for digital services

A report published by the **Belgian National Social Security Office** ([41]) highlights that chatbots offer significant advantages, such as providing clients with 24/7 responses to frequently asked questions, **reducing the workload** of contact centre staff and **managing high volumes of queries** during peak periods, thereby preventing queues.

However, the use of chatbots presents some challenges, particularly regarding the handling of personal data and ensuring data protection. Additionally, **there are limitations of artificial intelligence in understanding complex language**, such as technical terms used in the case of social security coordination. For example, the **Lithuanian National Health Insurance Fund** reported a bad experience with multilingual automated translations due to the poor quality of the services and misleading translations when these tools were incorporated in its online platform, leading it to no longer use them.

This issue highlights the fact that, while **automated translation plug-ins** for web browsers can be a useful tool for enhancing user accessibility to websites with limited language options, verified translation of digital services is crucial to ensure accurate and reliable information provision to citizens.

Instead, **several countries rely on human intermediaries for language support**. For instance, Austria's health insurance system offers personal service in multiple languages, including Romanian, Serbian and Turkish, while France maintains a database of staff with various language skills to provide support in users' native languages. In Slovakia and Finland, interpretation support services are available via telephone.

No Member State acknowledged significant issues with regard to **user satisfaction** with language options. However, assessing the effectiveness of multilingual support services is challenging due to limited data. Nonetheless, several **challenges** in providing effective multilingual support have been identified. These include limited language skills among staff, particularly noted by France and Poland, for handling documents in foreign languages, technical limitations in integrating multiple languages into existing digital infrastructures, and the need to balance the cost of developing multilingual services with the perceived low demand in some countries. For instance, Finland acknowledges that demand for non-Finnish-language services is currently very low, which may affect the perceived need for further development of multilingual tools. Similarly, in Iceland and Sweden, expanding multilingual services is not a priority in terms of investment due to the low volume of cross-border requests.

3.1.4. Accessibility challenges for cross-border users

The implementation of robust digital security measures is crucial for safeguarding user data and maintaining system integrity (see Section 3.4). However, these measures may also present accessibility challenges, particularly for cross-border users and non-residents.

Typically, there is **no specific portal dedicated to cross-border users**. This means that all citizens, whether working domestically or abroad, must submit their claims through the same online access point. Member States have reported that **one of the most significant challenges is the stringent eID and login requirements for users**. While these systems are vital for ensuring security, services that are not specifically tailored to the needs of mobile citizens may create barriers to accessibility, especially for cross-border workers and non-residents.

More specifically, many countries' reliance on national eID systems for authentication within social security online platforms has been reported to exclude groups of workers who do not have the required national credentials. This problem was reported in the majority of Member States and across social security branches. The following are examples.

- Finland allows users to access the online services of the Social Insurance Institution of Finland (Kela) through various eID methods, including Finnish bank credentials, certificate cards and mobile certificates. However, the Finnish Centre for Pensions utilises the Finnish national identity-matching service (a combination of eID and national personal identity codes), which is not able to effectively authenticate cross-border users' identities. Similarly, foreign employers seeking AWOD reimbursements through the TVKportal face barriers due to the system's reliance on Finnish bank credentials – a legacy of the traditionally domestic-focused process used by Finnish employers to handle compensation claims.

([41]) RSZ, *De RSZ: Geld, gegevens en sociale zekerheid*, Brussels, 2020, https://news.belgium.be/sites/default/files/news-items/attachments/2020-02/dossierPresse_170220_nl_v4.pdf.

- In Norway, users who do not have a Norwegian personal identification number are required to apply for family benefits on paper, effectively limiting access for non-residents. This lack of accessibility for migrant workers, particularly those not residing in Norway, is a known issue, which was exacerbated during the COVID-19 pandemic.
- While Danish citizens and those from eIDAS-supported Member States can easily update their information and request benefits online, users from unsupported countries still face challenges and must rely on manual processes ([42]).

It is worth mentioning that the complete implementation of the eIDAS regulation and EU Digital Identity Wallet, the full implementation of which is expected by 2026 ([43]), will enable citizens from all Member States to use a single, secure digital identity to access online social security services across Member States. This will streamline authentication, allowing users to prove their identity and access benefits more easily, while enhancing security and reducing fraud through standardised, high-assurance identification methods. Many social security institutions noted that the current shortcomings identified with national eID schemes will be solved by the implementation of the EU Digital Identity Wallet (Box 8). Flexibility with e-login options for online services will nonetheless be required to accommodate non-EU mobile citizens seeking to claim the benefits that they are entitled to in Member States.

Box 8. Implementation of the EU Digital Identity Wallet by 2026

The **EU digital identity (EUDI) regulation** ([44]), which entered into force in May 2024, builds on the eIDAS regulation, establishing a secure and interoperable digital identity framework across Member States for e-government services. A central feature is the **EU Digital Identity Wallet**, which streamlines identity verification to facilitate the application of the 'once-only' principle, reducing the administrative burden on and supporting cross-border user accessibility for EU citizens. In practical terms, the wallet will be a mobile app enabling users to identify themselves to public and private online services all over Europe. In addition, users will be able to **store, present and share digital documents** (everything from university diplomas to train tickets), as well as **electronically sign** or seal documents ([45]).

However, standardised forms of eID also **enhance data security**, reducing the risk of breaches by mandating cyber-security compliance. Additionally, it supports the **issuance of electronic attestations by public bodies**, fostering pan-European recognition of electronic credentials while ensuring data privacy. The EUDI regulation requires Member States to offer at least one EU Digital Identity Wallet to all citizens, residents and businesses by 2026.

The EUDI regulation is in synergy with three other EU projects dedicated to digitalising users' interactions with public administration in the social security field.

- The **Digital Credentials for Europe** (DC4EU) project ([46]) focuses on supporting the implementation of the eIDAS regulation and the SDGR by testing interoperability and scalability in the national domain and multiple cross-border contexts. In particular, work package 6, which is dedicated to the social security domain, involves the execution of large-scale pilots in a pre-production environment, which will contribute to the development of the capabilities of the EU Digital Identity Wallet, thus facilitating the implementation of the wallet in the Member States, especially in the social security domain.
- The EUDI regulation is also supported by the European blockchain services infrastructure **(EBSI)-Vector** project ([47]), focused on public sector blockchain services. The goal of work package 5 is to introduce and implement digital and decentralised concepts within the social security domain through the adoption of an EBSI-compliant wallet.

([42]) Interview with Udbetaling Danmark (8 July 2024).
([43]) The EU digital identity framework regulation (Regulation (EU) 2024/1183) amends the previous EU digital identity framework regulation (Regulation (EU) No 910/2014) as regards establishing the European digital identity framework. Member States are required to offer at least one EU Digital Identity Wallet to all citizens and residents by 2026.
([44]) Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European digital identity framework (OJ L, 2024/1183, 30.4.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32024R1183).
([45]) European Commission, 'The EU digital identity framework regulation enters into force', European Commission website, 21 May 2024, https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/The+Digital+Identity+Regulation+Enters+into+Force.
([46]) DC4EU commenced in April 2023, for a period of two years. For more information, see https://www.dc4eu.eu/project/.
([47]) For more information, see https://www.ebsi-vector.eu/en/.

- Results of DC4EU and (EBSI)-Vector project will be essential for next steps in the ongoing **ESSPASS** ([48]) project. This initiative is piloting the development and implementation of digital solutions to facilitate the interaction between mobile citizens and national authorities to improve the exercise of social security rights across borders. ESSPASS looks to make real-time verification of social security coverage and entitlements possible, including by those actors who do not have access to the EESSI system. The first phase focused on the cross-border digital verification of the validity and authenticity of A1 PDs. The second phase of the pilot, which is currently under way, is geared towards the issuing and verification of A1 PDs and EHICs.

Aside from secure online authentication, other barriers to user accessibility include **low awareness among users of digital options and procedures** (Denmark) and the **requirement for cross-border users to attend in-person to meetings at local offices**, either to verify personal information when this cannot be retrieved from national registries (Czechia: family and unemployment benefits) or to obtain the electronic certificate needed to interact with online services (Spain).

3.1.5. Digital maturity assessment and areas for improvement

Member States have demonstrably achieved **significant progress** in this dimension of digital maturity. The EU-wide implementation of accessible and comprehensive **online services for requesting PDs or claiming social security benefits** can be largely linked to the implementation of two key EU regulations, notably the SDGR and the eIDAS regulation. As part of the implementation of the former, Member States are required to ensure that citizens and businesses can access and complete various administrative procedures fully online and receive the output electronically. Several of these procedures relate to the social security coordination area, for instance: the request to determine which social security legislation covers the holder (the output of which is PD A1), applications for the EHIC, claiming pensions, requests for data on pensions from compulsory schemes and registrations with insurance schemes. On the other hand, the eIDAS regulation creates a cross-border legal framework that ensures the interoperability of eID systems in all Member States.

In line with the ongoing implementation of the abovementioned regulations, all countries reported having **online portals for mobile users** to gather information on and initiate application requests for either PDs or social security benefits. The variation in Member States' approaches to offering digital services therefore lies in the degree to which EU requirements have been implemented and extended to a wider scope at the national level. For example, fully digitally mature services in this dimension should support **user authentication mechanisms that are not strictly linked to national contexts** (in line with the eIDAS regulation's requirement of interoperable national eID schemes). To further amplify accessibility, they should offer users the possibility to consult information on how to complete authentication procedures in different languages beyond the official language(s) of that Member State. Box 9 sets out the key benefits of accessible digital services.

Member States can be divided into two main groups of digital maturity in this dimension:

- **Partially accessible digital services.** In all Member States, online portals are available to cross-border users, providing information on social security entitlements and application procedures across almost every branch of social security. However, the application process is partially digitalised, for instance due to application forms being in PDF formats that users are required to download, complete and re-upload to the social security portal. Similarly, although applications can be made online, PDs are only issued in paper format and sent to the client via post, which can slow down the process and be inconvenient for those who regularly change address. Additionally, some key services, such as updating personal information, cannot be completed online by users. National portals are not available in multiple languages beyond the official language(s) of the Member State, creating potential hurdles for non-native users. However, external content translation plug-ins remain available for the automated translation of web pages. Finally, while eID services are supported for online authentication to initiate a benefit request or document application procedure through the portals, local credentials are required, potentially excluding users who do not have residency in the Member State where they are making their social security service request.
- **Highly accessible digital services.** In some Member States, such as Finland, Norway and Slovenia, cross-border users can complete administrative procedures through online portals for nearly every branch of social security. Online forms on such portals automatically pull data from relevant registries to prefill applications with relevant information (e.g. personal data) and ensure that all relevant criteria are submitted before an application can be completed. Moreover, digital services are offered in multiple languages targeted at the main groups of cross-border users, with chatbots for information or further support. Communication with social security institutions is encouraged through digital means, including automated notifications of users' application status. Furthermore, users are able to update their

([48]) ESSPASS was launched in 2021 and will conclude in 2025. For more information. see https://ec.europa.eu/social/main.jsp?catId=1545&langId=en.

personal information online and receive digital copies of the PDs issued to them. All of these factors facilitate users' remote access to national digital services, allowing mobile workers to claim the social protection that they are entitled to from any location. Importantly, paper-based applications remain an option, to ensure that no citizen is excluded from digitalisation initiatives due to a lack of digital literacy or limited access to information and communications technology (ICT).

Box 9. Key benefits of accessible digital services

Accessible digital services **enhance the uptake of social security benefits** and **protect workers' rights** by providing clear, user-friendly information and streamlined application processes, thus empowering individuals to better understand and claim their entitlements.

This is particularly key with regard to the **inclusion of key vulnerable and minority groups**. Full digital maturity in this dimension should therefore also include services' compliance with Directive (EU) 2016/2102 on the accessibility of public sector bodies' websites and mobile applications and with Directive (EU) 2019/882 on the accessibility requirements for products and services, which sets out specific accessibility and inclusivity requirements in Annex I. Furthermore, in line with the European declaration on digital rights and principles for the digital decade ([49]), digital maturity should ensure that no citizen is excluded from the provision of social security services due to a lack of digital literacy or limited access to ICT, meaning that client support services and alternative communication channels should be made available in parallel.

Moreover, accessible digital social security services **facilitate the employment of cross-border workers** in the EU by providing employers with streamlined and predictable application procedures, reducing administrative burdens and enabling smoother onboarding processes across different countries.

The main gaps that remain, and which should be addressed to achieve full digital maturity across the EU with regard to the accessibility of digital social security services, are the following:

- **Integration of the eIDAS regulation** (the full implementation of which is expected by 2026 ([50]). This is a crucial step to allow cross-border users to access online services using secure authentication mechanisms that are not exclusively linked to local credentials. In this way, mobile users can claim benefits or make requests from social security institutions in countries where they have previously worked or lived, regardless of their current residency or citizenship status.
- **Updating personal information.** Enabling mobile users to promptly update their personal information in cross-border social security systems minimises errors, reduces fraud risks and improves user experience. This streamlined process facilitates efficient administrative procedures and information exchange between social security institutions, while reducing the risk of conflicting data in various systems.
- **Language accessibility.** Implementing multilingual platforms and chatbots for national social security portals and websites ensures equitable access to services for users, breaking down language barriers and enabling citizens to navigate complex social security systems in their preferred language. This is in addition to the legislative requirements in EU law ensuring that all EU languages can be used for certain purposes (e.g. filing applications or other documents).
- **Issuing digital versions of documents.** Issuing digital documents via online portals or secure email, rather than relying on paper versions sent through postal services, is an important aspect of accessibility, as it ensures faster delivery, reduces the risk of loss or delay, allows immediate access and facilitates document verification. One key example of this is the project to digitalise the EHIC, which is currently being undertaken by the Administrative Commission for the Coordination of Social Security Systems. Notably, digital documentation should be developed with strong authentication measures (e.g. trust credentials or QR codes for validation) to prevent digital forgery (see Section 3.5).

([49]) European Commission, European declaration on digital rights and principles for the digital decade, Chapter II – Solidarity and inclusion (OJ C 23, 23.1.2023, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001).

([50]) The EU digital identity framework regulation (Regulation (EU) 2024/1183) amends the previous EU digital identity framework regulation (Regulation (EU) 910/2014) as regards establishing the European digital identity framework. Member States are required to offer at least one EU Digital Identity Wallet to all citizens and residents by 2026.

- **Client support services and non-digital communication channels.** Online chatbots, frequently asked questions pages and/or telephone helplines to support clients in navigating their digital journey when applying for social benefits or PDs online are important to ensure that no citizen is excluded from the provision of social security services due to a lack of digital literacy. Similarly, alternative communication channels should be kept open between social security institutions and citizens who do not have access to ICT. Continuing to accept paper-based applications is crucial in this regard.

3.2. Digital administration (management of claims and granting of benefits)

Key findings from this section: digital administration across Member States

Digital maturity in this dimension across the EU can overall be considered:

PARTIAL

Member States show extreme variance in the degree to which request handling is digitalised or automated by social security authorities. Only a handful of social security bodies in the Member States have fully automated their internal procedures by employing algorithms to complete decision-making or administrative tasks. However, cross-border cases are typically complex and therefore require human intervention.

Importantly, all institutions with automated processes (e.g. back-end checks or decision-making algorithms) employ 'semi-automated procedures' when it comes to issuing PDs or granting benefits, whereby automatised processes are combined with some form of human oversight or intervention. There is also a growing trend across the Member States of digital communication with end users through online social security platforms, allowing direct, secure interaction with relevant authorities that might need to request additional information or send out procedural notifications to their clients.

The key benefits of digitalising administration systems include increased efficiency, reduced errors, better handling of high volumes of requests and freeing up resources to focus on more complex cases, thereby improving public services – all of which are crucial as the EU promotes cross-border labour mobility.

There are key gaps that need to be filled to harmonise Member States' digital maturity in this dimension. These include widespread implementation of automatic verification procedures for eligibility checks and automated calculations of due benefits, as well as the use of digital document management systems.

Social security authorities are increasingly digitalising procedures to streamline the process of granting benefits or relevant social security documentation (e.g. PDs) to mobile citizens. By adopting digital tools and platforms, authorities can ensure **quicker processing of applications**, **minimise bureaucratic complexities** and **reduce the likelihood of human errors**. Automation also helps **handle high volumes of requests**, providing a more consistent and transparent service. This modernisation reflects a commitment to using technology for more effective public services as the EU continues to foster cross-border labour mobility.

Various institutions in several Member States and social security areas recognise the impact of automation in speeding up digital administrative processes.

- In Czechia, Denmark, Finland, Germany, Iceland, Lithuania, Malta, Norway, Slovakia and Slovenia, the introduction of digitalised procedures has reportedly led to a **reduction in the duration of procedures in the area of applicable legislation and pensions, as well as savings in human resources**. In Czechia, for example, process automation has led to faster procedures, fewer staff and greater accuracy in the process. In Denmark, digitalisation has also allowed caseworkers to focus on more complex tasks, thereby improving service quality by automating routine tasks. Finland reports that the automation rate of PD A1 procedures has increased from 25 % in 2018 to 65–70 % currently, with a decrease in processing times from 45 to 16 days. In Iceland, linking the database to internal systems has reduced case processing time from three weeks to one week.
- Looking instead at **sickness benefits**, the benefits of automation are well recognised in Czechia, Lithuania and Norway. In Lithuania, digitalisation has enabled 19 000 procedures to be checked and paid by a single person. At the same time, automation was considered useful during the outbreak of COVID-19, when several people were stuck abroad and needed proof of health insurance if they needed medical assistance.

- In the area of **unemployment and family benefits**, positive experiences are reported from France, Luxembourg, Malta and Poland. In France, for instance, the automation introduced by the Eureca application shortens and facilitates repetitive and tedious tasks, while limiting errors.

3.2.1. Digitalisation of documents

The vast majority of Member States reported making use of digital documents throughout the benefit application processing procedure. Three main forms of digitalisation of documents were identified:

- A number of Member States reported having set up **specific procedures for scanning paper documents and/or producing digital documents from claimant application forms** (automatic document recognition/reading (RAD/LAD) systems), after which they are electronically transmitted to caseworkers. This is the case in Belgium, Czechia, Denmark, France, the Netherlands and Slovenia. For instance, in Denmark, Udbetaling Danmark uses automated data capture software (named Tungsten Automation ([51]) to scan documents. The documents are then subject to registration so that the individual document can be handled by the relevant caseworkers. Belgium reported the use of robotic process automation (RPA) for developing a bot that carries out the automatic uploading of a large number of documents to the electronic document management system ([52]).
- A few Member States reported using more comprehensive **digital document management systems**. This is, for example, the case of Croatia and Slovenia. In Slovenia, the ZPIZ employs a digital document management system into which paper documents are received and then promptly scanned and incorporated into automated electronic workflows. The ZPIZ generates and stores all outgoing documents in a digital format. The system implements a verification process for incoming documents, encompassing structure and digital signature validation. In Croatia, the Pension Insurance Institute employs a document management system that generates QR-coded electronic documents for verification. Such digital document management systems may be part of a fully digitalised benefit application processing system (see Section 3.2.2).
- A few Member States have implemented **automated verification procedures of social-security-related documents**, such as the verification of signatures for authenticity, assessing content and timestamping (Box 10). Such initiatives are most often set up as pilot projects and are not yet widely implemented in any of the countries investigated. Moreover, they are most often not specific to mobile workers but are implemented at the level of the organisation, which ensures social security coverage for both static and mobile citizens.

Box 10. Good practice: automated verification of digital documents in Spain and Slovenia

In **Spain**, the Digital Transformation Office – the digital transformation area of the social security IT department – is currently testing a pilot project using artificial intelligence for the validation of administrative files. This project focuses on processing and classifying documents submitted electronically by citizens and extracting the necessary information using artificial intelligence. The social security IT department is responsible for digitalisation aspects regarding pension, unemployment, sickness, family, AWOD, maternity and paternity benefits.

In **Slovenia**, the ZPIZ has implemented fully automated verification for documents received via external channels, involving schema validation, electronic signature verification, content assessment against predefined business rules, timestamping and preparation for long-term electronic archiving.

A few Member States have integrated digital translation tools for the **automatic translation** of documents received in foreign languages by cross-border users in their internal data management systems (Belgium and Finland). For instance, Kela in Finland uses an internal, secure translation machine (Tilde) that translates approximately 15 different languages into Finnish, to support case officers with the interpretation of foreign documents. Other institutions (e.g. the Belgian Federal Agency for Occupational Risks) noted that they use encrypted and secure translation software such as DeepL ([53]) for translating documents.

Other countries have not yet implemented automatic translation instruments for different reasons. In Norway, the use of online artificial intelligence (AI)-powered translation tools is prohibited within the institutions due to concerns related

([51]) See https://www.tungstenautomation.com/.
([52]) RSZ, *De RSZ: Geld, gegevens en sociale zekerheid*, Brussels, 2020, https://news.belgium.be/sites/default/files/news-items/attachments/2020-02/dossierPresse_170220_nl_v4.pdf.
([53]) See https://www.deepl.com/en/products/translator.

to protecting the personal data of clients. In the Netherlands, similar concerns were raised regarding the integration of automated translation tools, along with concerns about the insufficient maturity of such technologies and the risk of errors. Indeed, several countries highlighted that ensuring the use of precise and appropriate terminology is a key obstacle when dealing with cross-border cases.

3.2.2. Automation of benefit-granting procedures

The degree to which the processes for verifying applications and allocating benefits are digitalised within social security institutions is varied. Often, automation varies based on the eligibility requirements and vetting procedures associated with those specific benefits. Indeed, the benefit evaluation and granting procedure looks different across social security branches.

Applicable legislation

The analysis of automated processing in handling requests related to applicable legislation (notably A1 PDs) reveals varying levels of automation and digitalisation across Member States.

Several Member States (e.g. BE, FI, LT and NO) report having introduced **advanced automated systems** for determining the applicable legislation, generally with some limited form of human intervention. The Working Abroad service provides users with the possibility to obtain an A1 document in 12 to 24 hours through an automated verification procedure (accounting for 80 % of the cases). If the automated verification fails, a caseworker will intervene, who will most likely solve the issue in two to three days. In Finland, 90 % of A1 applications are submitted electronically and 65–70 % of these are processed through the automated system, with an average processing time of 16 days (across both manual and automated procedures). In Lithuania, A1 applications are done through specific portals (EDAS for companies and EGAS for employees, who can also submit claims in paper form). Box 11 outlines the automated processing of PD A1 applications in Norway.

Other countries are also making **progress in digitalising the application of A1 documents and their verification, although are still relying significantly on human verification**. For example, in Portugal, A1 PDs carry a code that clerks must enter in the social security website to verify their authenticity. Moreover, in Iceland, the issuance of A1 PDs is mostly solved electronically, but the determination of applicable legislation is largely performed manually. In the Netherlands, employers and employees can apply for A1 PDs digitally via a portal. Roughly 60 % of applications done by employees are processed automatically if the details are correct.

Some countries reported having implemented the **automation of EESSI cross-border notifications concerning A1 PDs**. This is the case of Germany and Italy. To process incoming A1 PDs issued abroad, instead of manually checking all incoming information according to proposed legislation, the automated procedure grants a maximum processing time of 48 hours.

Box 11. Good practice: automated processing of cross-border PD A1 applications in Norway

In Norway, the Altinn digital portal serves as the platform for submitting claims and documents to various governmental authorities. A portion of the information required to determine the applicable legislation is **automatically prefilled** from public registries. The employer completes the remaining sections of the form without access to the prefilled information, thereby safeguarding the privacy of the individuals involved. Once the form is completed, the case management system retrieves the necessary information directly from the application and integrates it into the **case processing system**. Consequently, when all of the information has been verified, the A1 certificate is issued directly to the end user via post, with a copy sent to the employer.

One key challenge, flagged by the Belgian National Social Security Office's applicable legislation division, is **the issue of accessing data registers for employers without formal registration in the country**. For Belgian-registered employers, which are already integrated into Belgium's national data systems with registration numbers, the system allows essential employment-related data to be automatically verified. However, foreign employers – particularly those without registration in Belgium and operating on a temporary basis or in sectors such as seasonal work – do not have the same streamlined access to these systems. This complicates their ability to manage employee-related tasks, such as reporting wages, confirming employment status and processing social security contributions.

The goal is therefore to link all relevant employment data (e.g. wages, contracts and social security information) to a centralised system that minimises the need for redundant information requests. However, providing access to these data for unregistered foreign employers is complex, as they may not have the same rights as Belgian entities. At the same

time, Belgium cannot mandate registration for foreign employers who have no obligations under Belgian social security legislation, as this would infringe on the freedom to provide services across borders. Therefore, while registration remains an option for those with sufficient cause (e.g. employee being subject to Belgian legislation), it cannot be imposed, complicating access to data for foreign entities. This presents significant challenges due to the intricate balance between ensuring secure access to sensitive data for social security coordination across borders and adhering to legal frameworks that protect freedom of movement and services in the EU.

Maternity/paternity benefits and family benefits

Most countries reported **partial implementation of automated procedures** for issuing maternity/paternity and family benefits for mobile workers. The reasons for the lack of automation in the issuing process of these types of benefits differ across countries.

- **Complexity of cross-border cases.** While national applications are often fully automated, cross-border complexity typically requires manual intervention, such as verification of eligibility or consultation with the applicant. Automation is used to a lesser extent, as the complexities of international cases often present practical challenges that are difficult to automate. For instance, in Norway, the process for universal child benefits is fully automated for children born within the country, while parents of children born abroad are required to submit an application. In cross-border cases, the initial steps involve manual verification of claims, but once these are confirmed, the process proceeds similarly to the automatic system in place for children born in Norway.
- **Greater need for data exchange.** While national authorities generally have direct access to their own databases, **cross-border cases necessitate requests to foreign institutions**, which can slow down the process due to the increased complexity of cases and the need for additional data. The only institution reporting the existence of a data-exchange agreement with another country for family benefit is the French Family Benefit Funds (Caisse d'allocations familiales (CAF)), which has an agreement with Luxembourg that complements data exchanges via EESSI (Box 12).
- **Differences in legislation and currencies.** The reliance on manual checks is further compounded by differences in legislation and currencies, which make fully automated decisions impractical. The competent Finnish institution argues that different currencies complicate automated decisions being made.
- **Coordination required between institutions for the verification of eligibility.** Coordinating among different Member States' institutions complicates the automation of cross-border cases. In Finland, determining whether a child qualifies for residence-based social security must be resolved manually before a decision on benefits can be made. Similarly, in the Netherlands, the recognition and validation of relevant forms and documentation from non-EU countries necessitate expert review, as automation alone cannot handle such complexities.

Box 12. Good practice: digitalisation initiatives in the field of family benefits in France

Bilateral data-exchange agreements

In France, CAF utilises an **integrated system** for exchange of digital documents and information on beneficiaries' rights with Luxembourg. To simplify document exchanges, information on family benefits is **digitally communicated via an online portal** to the Luxembourg authorities. However, Luxembourg is the only country with which such digital communication is in place.

According to CAF, a similar project is currently being considered with Switzerland. Experience from its collaboration with Luxembourg reveals that the completion of the project relies on the **mutual maturity of the internal information systems**. Notably, the systems of all authorities involved in the project must be coordinated and up to date to be able to align with those of the second country involved. Additionally, all authorities need to use the same versions of systems and the same tools for the project to succeed.

Based on the information provided, with all other Member States, the exchange of documents outside EESSI occurs on paper.

Recovery of outstanding benefits

The institution employs an automated system to detect and recover unduly paid benefits. Family allowance rights are **calculated automatically**, including adjustments for overpayments. Recovery of these payments can occur automatically only if the family allowance rights are still pending. **Notifications** for regularisation are also automatically sent to the beneficiaries. In practice, the system also allows all users to instantly know the benefits to which they are entitled to upon submitting their application.

Sickness benefits in kind and in cash

Looking at automation in handling requests for sickness benefits, a diverse landscape emerges.

Certain countries, such as Czechia, Denmark, Lithuania and Norway, display **fairly advanced automation in the processing of requests**. In Denmark, Udbetaling Danmark has implemented automatic handling of documents for 12 years. Applications are vastly automated for citizens living in Denmark and in possession of the country's eID (MitID). Information is regularly withdrawn from the tax agency to ensure the delivery of the correct amount of benefits. Norway has fully automated the EHIC application, with manual intervention required for a few cases, for postal delivery and for partially automated S1 and S2 applications. In Czechia, users are able to submit forms in the CSSA e-portal without logging in; authentication is required, however, for more advanced functionalities, such as automatic data loading for sickness insurance in cash and electronic sick leave. The CSSA operates around 100 internal IT systems and utilises a centralised application connected to various registries and databases to recover outstanding contributions and overpaid benefits ([54]). Meanwhile, Lithuania employs automated checks to verify insurance status and entitlement, with manual verification limited to more complex tasks, such as registering a person bringing an S1 from another Member State.

Other countries are **progressing towards greater digitalisation in the sickness benefit area**. The following trends have been identified:

- **Automation of the EHIC application process, but not for other PDs.** While the SDGR requires the EHIC application procedure to be digitalised, no other EU-level requirements exist for other PDs in the field of sickness benefits. Consequently, some Member States have not advanced in digitalising applications pertaining to this branch of social security beyond the SDGR obligations. This is the case of the following countries: Austria, Estonia, Iceland, the Netherlands and Poland.
- **Electronic issuance or storage of documents, but manual verification.** This is the case in a few countries. In Finland, PDs are issued electronically but they are not verified automatically (Box 13). In Malta, a cloud management system has been implemented in which documents are vetted manually but stored electronically, allowing users to upload missing documentation in the country's digital social security portal.

Finally, it is worth noting that **many countries rely exclusively on EESSI in their processes to facilitate secure and standardised information exchange in the sickness benefits domain**. This is the case, for instance, in Austria, Czechia, Denmark, Lithuania, Luxembourg, Malta, the Netherlands, Norway, Poland, Portugal and Sweden.

Box 13. Good practice: automated processing for cross-border PD S1 applications in Finland

If a client, such as a pensioner, plans to relocate to another Member State, they must apply to Kela for a PD S1. The application may be submitted in paper form or **completed online** via the OmaKela platform.

Upon receipt of the application, Kela processes it using its **benefit processing system**, known as Onni. This system evaluates the applicant's eligibility by **verifying conditions** such as other benefits the individual may be receiving, their inclusion in the residence-based social security scheme and any relevant pensions or daily allowances. While much of the benefit information is **retrieved automatically** from national registers, a human clerk may be required to input certain details, particularly where foreign benefits are concerned, based on information provided by either the client or another institution. The system **cross-references the benefit data** with the applicable time period and the applicant's status. Thus, although parts of the process are automated, the involvement of a clerk remains necessary throughout.

Should the applicant be deemed eligible for healthcare and the issuance of a PD S1 is required, the form is generated at the time of the decision. The system programmatically determines the need for the form, which is then automatically generated. A clerk prints the certificate, affixes the necessary stamp and signature, and dispatches it to the client. If the client has opted out of receiving physical mail, **they will receive their benefit decision and any necessary PD forms electronically** via OmaKela.

Following the application phase, the registration phase commences. This phase is managed through EESSI between institutions, once the client has presented the S1 form to the relevant institution in their new country of residence. In some instances, the process may begin directly with EESSI, for example if an institution from another Member State submits structured electronic document S071, requesting an entitlement certificate (S072). In this scenario, the certificate is not issued as an S1 form but is **delivered electronically to the requesting institution**. The same procedures and inferences are made in the benefit-processing system as in the S1 case.

([54]) Czechia is the only country reporting automation for the recovery of unduly paid benefits in the sickness benefit domain.

Accidents at work and occupational diseases

For AWOD, there is in general no automated processing reported by competent social security institutions in any of the Member States. One exception is Luxembourg, where DA1 PDs are automatically forwarded in a digital format by the Association d'Assurance Accident to the relevant social security institution upon receiving an accident declaration from employers. Additionally, a paper copy of PD DA1 is dispatched to the insured person. This process is carried out proactively, without the need for a formal request for the PD, ensuring that PD DA1 is issued as quickly as possible. However, any subsequent requests attached to a single case, such as requests for duplicates or date extensions, are processed manually by a case officer.

Unemployment benefits

There is significant variance in the degree of automation implemented by institutions responsible for unemployment benefits in Member States. Notably, EESSI was the most cited channel for data exchange and form of automation in the field of unemployment benefits.

Some Member States reported **introducing significant automation into the processing of unemployment benefit claims**. For example, Kela in Finland, the Belgian employment service and the Dutch Employee Insurance Agency have developed advanced automated data-processing systems for the calculation of unemployment benefits, with automated subprocesses and decisions used to calculate the correct amount of benefit. For instance, in the Netherlands, authorities have the full history of workers who live in the Netherlands and have a citizen service number. For this reason, however, the degree of automation for workers who live abroad is lower, since their work history is added manually.

In some countries, **automatised vetting of claims is combined with human intervention for verification purposes** (DK, DE, LU and MT). Human intervention might occur in different ways. The German Federal Employment Agency primarily uses automation as a support tool, with human intervention required for the final decision due to cash-handling regulations. Similarly, in Luxembourg and Malta, human verification of automated processing is required, even if the system responds positively. In Denmark, automated checks handle identity, eligibility and completeness, but caseworkers verify subsequent changes or flagged exceptions. Luxembourg and Malta rely on automated systems for initial processing, but manual verification is required for flagged issues or to finalise document approval (Box 14), such as with PD A1 and U1 forms in Malta.

The benefits of integrating digital interinstitutional communication systems also at the national level were highlighted in Hungary, where the central employment office need to liaise with district departments for the handling of unemployment cases, since the latter are better placed to verify information on clients and relevant employers.

Box 14. Good practice: introduction of automated processing for unemployment benefits in Luxembourg

Currently, the process for requesting unemployment benefits is largely manual in Luxembourg, requiring multiple paper-based forms to be completed by the jobseeker, which are reviewed by the Agence pour le Développement de l'Emploi and then digitalised by a dedicated scanning team. After further manual checks and validation from authorised clerks, the jobseeker is subsequently informed of the outcome via email. Due to inefficiencies, the process is currently undergoing major digitalisation.

In the future, once an individual registers as a jobseeker, they will receive a link through which they can submit a **digital application** for unemployment benefits via the MyGuichet platform. This will involve completing a questionnaire, confirming the submission and providing the necessary supporting documents through the new business application. In this updated process, the form will be **prefilled**, and a **simulation of the benefits** that are to be received will be available. For more complex cases, a second review involving human intervention will be conducted. Following this, a decision will be made, and the jobseeker will **receive a grant letter digitally**, with a notification sent through the application.

The objective is to centralise all processes within MyGuichet, with a dedicated front-end space referred to as MyADEM. At present, this system applies only to full unemployment benefits. Upon submitting an application, a jobseeker's MyADEM space is automatically created on the MyGuichet platform. Simultaneously, a new back-end system will be utilised by the administration for **file processing**. In the future, if an application is incomplete or presents an issue (e.g. the recovery of overpaid contributions), an **automatic alert** will be generated. Reminders will also be automated when there has been no response from the jobseeker.

Pensions

The field of pension benefit coordination has seen significant integration of automated procedures across Member States. These advancements aim to streamline processes, improve efficiency and enhance the accuracy of benefit calculations and disbursements.

Many pension authorities have implemented **automated systems for calculating due benefits and verifying digital documents**. However, it is important to note that, despite the implementation of such advanced digital tools, **most pension authorities emphasise the necessity of human intervention**, such as in Denmark, Ireland, Portugal and Finland (Box 15). Clerks' approval is typically required before a decision is rendered final to the client, ensuring a balance between automation and human oversight.

Box 15. Good practice: combining automation and human oversight for cross-border pension coordination in Denmark, Ireland, Portugal and Finland

The recent entry into force of the EU AI Act (Regulation (EU) 2024/1689) ([55]) underscores the critical concept of 'human in the loop', which describes a collaborative approach whereby human input and expertise is maintained throughout the life cycle of machine learning and AI systems. Article 14 of the AI Act required high-risk AI systems to integrate human oversight in an appropriate and proportionate way ([56]).

In **Portugal**, the 'pension on time' application is an automated component of the wider integrated system of pensions, which is used to register and analyse pension applications. 'Pension on time' means that people who meet all the conditions for retirement, when they reach the legally required age, do not have to wait for the analysis of their pension request by an employee to start receiving the old-age pension. However, verification of the documentation that is attached to the pension application still needs to be confirmed by an employee ([57]).

In **Denmark** and **Ireland**, authorities' administrative systems undertake automated checks for completeness and accuracy of applications. Digital handling procedures include automated data entry, validation and routing of documents to the appropriate departments. Automated checks include verifying the user's identity and eligibility and the completeness of the application made by the user online through the national portal. If all criteria are met, the system can approve the application automatically; however, this decision needs to be approved by a caseworker before a PD P1 (Denmark) or PD A1 (Ireland) is issued to the client. All subsequent changes in the system will be checked by a caseworker.

In **Finland**, earnings-related pension institutions have also automated the processing of pension applications and the decision-making related to them. The Finnish Centre for Pensions uses certificates and identification/security standards that categorise information/documents to verify a person's identity or that the information coming from an institution is validated. The Finnish Centre for Pensions' processing systems also automatically provide personal and benefit data to the clerks from register data interfaces. In Finland, register data are used extensively, within the framework of clerks' information access roles.

While certain parts of internal business processes are automated in the field of pension benefits, **procedures in cases with a cross-border element cannot be automated to a greater extent**. Much like for other branches of social security, the full integration of automated procedures in cross-border cases is largely dependent on the accessibility of other Member States' pension databases. The exchanges via EESSI are mostly manually handled and often take time to complete. While some countries have established bilateral agreements to share death data of pension beneficiaries (see Section 4.3), the

([55]) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (OJ L, 2024/1689, 12.7.2024, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689).

([56]) Recital 58 of the AI Act (Regulation (EU) 2024/1689) states: 'Another area in which the use of AI systems deserves special consideration is the access to and enjoyment of certain essential private and public services and benefits necessary for people to fully participate in society or to improve one's standard of living. In particular, natural persons applying for or receiving essential public assistance benefits and services from public authorities namely healthcare services, social security benefits, social services providing protection in cases such as maternity, illness, industrial accidents, dependency or old age and loss of employment and social and housing assistance, are typically dependent on those benefits and services and in a vulnerable position in relation to the responsible authorities. If AI systems are used for determining whether such benefits and services should be granted, denied, reduced, revoked or reclaimed by authorities, including whether beneficiaries are legitimately entitled to such benefits or services, those systems may have a significant impact on persons' livelihood and may infringe their fundamental rights, such as the right to social protection, non-discrimination, human dignity or an effective remedy and should therefore be classified as high-risk.'

([57]) Instituto da Segurança Social, 'Pensão na hora' ('Pension at the time'), 2021, https://www.seg-social.pt/noticias/-/asset_publisher/kBZtOMZgstp3/content/pensao-na-hora.

cross-checking of these databases within internal systems often still requires human intervention. For example, in Norway, if all information is available in the registers of the national insurance administration, the pensions claim made via the online portal by a given user is processed and the answer is sent electronically, including the calculation of the pension, in less than 30 seconds. This is a wholly automated process. If additional information is needed (e.g. information on pension rights from another Member State), the process is semi-automated: in other words, it is put on hold until the additional information has been received. The rest of the process is then completed automatically. Box 16 gives a further example from Hungary.

Box 16. Good practice: automated processing for cross-border pension benefit coordination in Hungary

The determination of Hungarian social security benefits generally requires human evaluation of eligibility conditions. However, several automatic mechanisms are in place to support the process. For instance, electronically received applications are **automatically registered** in appropriate subsystem registers. Applications received through EESSI are processed by robots, and **summaries are generated** to facilitate easier processing.

Automation also affects benefit payments. For pension matters, data from employers, tax authorities and other bodies are **automatically added to the relevant electronic case file**, eliminating manual data entry. For instance, student status for orphan's benefits is **automatically verified** by the paying agency using data from public education and vocational training registers. Hungarian benefits are also **automatically terminated** if the beneficiary passes away, as this information is transferred from the Hungarian personal data and address register to the paying agency. To this end, Hungary has established an **electronic data-exchange system** for pension beneficiary deaths with Germany. The exchanges occur via a **sPAD application/server which is developed by Germany**.

Additionally, communication between economic organisations and administrative bodies is primarily electronic. Document mailing for pension matters with clients, including envelope placement, is further handled through an automatic mechanism.

Finally, an automatic process allows clients to **check their case status** and obtain information about their benefits.

Additionally, some social security authorities make use of **automated procedures with financial institutions to support their administrative procedures regarding the recovery of unduly paid benefits**. Notably, automated and digitalised data exchange prevents unjustified payments, since pension authorities are able to obtain information about the death of beneficiaries from abroad significantly earlier than they would have without this automation and are able to take due action to terminate the payment of pension benefits.

- In Czechia, for the recovery of outstanding contributions and paid benefits, there is a centralised application interconnected with the relevant CSSA apps, registers and databases and governmental registers.
- In Portugal, when the date of death of deceased users who were pensioners is recorded by the institution, there is an automated calculation of unduly paid amounts. However, in some cases, user intervention is still required. Notably, when there are accumulations of benefits that should not be issued due to given circumstances, but the automatic pension-granting system 'pension on time' is unable to verify these situations, it can lead to the payment of undue amounts. These cases make up a small percentage and, therefore, the advantage of automation outweighs the inconvenience of dealing with benefit accrual situations.
- In Hungary, in cases involving the German–Hungarian death data exchange, if a beneficiary passes away, the payment of the benefit is automatically terminated. When unauthorised payments were made after the death, these are automatically collected to recover the overpaid benefits.

3.2.3. Digital communication with clients

Member States' social security institutions report the use of a variety of channels for communication with users:

- **Portals or dedicated channels.** Several Member States have implemented communication channels with users through **portals, dedicated channels or secured emails**, noting that such channels provide greater security for user communication. This is, for instance, the case of institutions in Czechia, Denmark, France, Germany, Iceland, Lithuania, the Netherlands, Norway and Portugal. In some of these countries, communication via emails is discouraged or not allowed, generally for data-protection reasons, and their use is limited to notifying users about a message received in the portal where the full information is made available (CZ, DE, LT and NO). In other countries, institutions, such as CAF in France, the Latvian National Health Service (sickness benefits) and the Dutch Employee Insurance Agency,

still allow email communication for correspondence with end users, in parallel with communication through the dedicated portals. Overall, user communication via platforms is **progressively expanding**. A number of institutions announced having similar initiatives in the pipeline or testing phases (e.g. the Belgian Federal Agency for Occupational Risk (AWOD benefits), CAK in the Netherlands (sickness and family benefits), the Employment Service of Slovenia (unemployment benefits) and in Luxembourg). Box 17 sets out good practices for fostering online communication.

- **More traditional communication methods.** Some Member States' institutions continue to use email for communication with end users. This is, for instance, the case of the Belgian organisation dealing with family benefits and the Bulgarian organisation for AWOD and sickness in kind. In the Icelandic Social Insurance Administration (pensions and applicable legislation), emails are used to send documents to users.
- **Multichannel communication.** Several Member States' institutions use multiple means of communication to ensure inclusivity and communication with more vulnerable groups, such as the elderly, or with citizens without access to the internet or who are less digitally proficient. For instance, in Portugal, alongside the e-clic portal, users can also communicate via phone and video calls. In the Netherlands, users also have the possibility to communicate via phone or in person in a customer attention centre.

Box 17. Good practice: fostering online communication between social security authorities and cross-border citizens

In **Belgium**, the Federal Pensions Service always provides citizens with the option of becoming a 'digital customer'. This means that, whenever a (digital) document or message is sent to users, they receive a notification by email inviting them to log in to mypension.be and view the message/document. However, if they do not feel comfortable with digital tools, all documents can be sent by post.

In **Czechia**, for pensions, applicable legislation and sickness benefits, the CSSA e-portal is the main electronic communication method, with emails used only as a supportive tool and considered not suitable for delivering decisions or handling protected data.

In **Germany**, the Pension Insurance Institute favours the use of the secure online service as a means of communication with end users from other Member States.

In **Lithuania**, communication regarding applicable legislation takes place via the EDAS (for companies) and EGAS (for employees) platforms, ensuring compliance with the requirements of the general data-protection regulation.

In **Norway**, portals are preferred across various social security domains, with paper communication employed as an alternative, since emails are not used for personal information.

3.2.4. Challenges with the automation of administrative procedures

Automation in digital administration involves challenges. The following are some of the challenges identified by the institution representatives interviewed:

- **Differences in the degree of digitalisation of purely national and cross-border situations.** In some Member States, these differences arise because some form of national identification is needed to access certain procedures (as in Norway and Poland). Another reason lies in the complexity of cross-border procedures (e.g. in Czechia and Finland), where issues such as different legislation or currency conversion might slow down processes, requiring more manual intervention (Finland). Looking at specific procedures, **only a few countries report automation in the recovery of outstanding contributions or unduly paid benefits**; this is the case of Czechia for pensions and of France for unemployment and family benefits, but in only certain situations in the latter. In Germany, automated recovery for unduly paid pension benefits has so far been implemented only at the national level, since, as the institution claims, there is no legal basis to do it internationally.
- **Low number of cross-border cases.** The low number of cross-border cases in some Member States may not encourage the adoption of context-specific automated procedures. This is the case of Poland, for example, where the digitalisation of handling S1 and S2 PDs is not planned because the number of requests is relatively low, with fewer than 100 000 cases annually. In Iceland, the payment of pensions to foreign accounts remains manual, since the low number of cases does not incentivise the development of automated systems. In Finland, A1 application procedures for seafarers and flying personnel are not automated due to their fairly low volumes.

- **Other challenges.** The CSSA in Czechia argues that, while automation has shortened processing times, it has also led to **more requirements on data and clerk skills**, with higher expenditures and greater coordination requirements (see Chapter 5 for further information). In Luxembourg, **previous bad experiences with digitalisation** have led to greater caution in implementing digital tools in the field of family benefits.

3.2.5. Digital maturity assessment and areas for improvement

Digitalised internal administrative systems offer significant advantages in managing cross-border workers' benefits and documentation. These systems streamline the process of granting benefits and issuing relevant social security documents, such as PDs, by leveraging digital tools and platforms. Such modernisation allows authorities to process applications more quickly and minimise human errors. Moreover, automation enables the handling of high volumes of requests, ensuring a more consistent and transparent service. As the EU continues to promote cross-border labour mobility, these technological advancements play a crucial role in enhancing the efficiency and effectiveness of public services, ultimately benefiting workers, employers and administrative bodies.

Digital administration therefore comprises introducing automated procedures to reduce bureaucratic burdens for caseworkers, enabling the faster handling of requests and freeing up internal resources to focus on resolving complex cases that require human intervention. As many social security institutions across the EU emphasised in their responses to this study, complexity is a recurring characteristic of cross-border cases in particular. Consequently, they often require caseworkers with expertise in cross-border coordination to settle pending issues that automated procedures cannot resolve.

Consequently, digitally mature administration infrastructure plays a crucial role in the EU's attempt to encourage cross-border employment and labour mobility while guaranteeing the efficient social protection of cross-border workers. Digital maturity in this dimension includes the implementation of digital document-handling systems for digitalising, exchanging and archiving documentation relevant to applicants' requests; automated procedures for application evaluation (e.g. translation tools for foreign documents and automated verification of information through back-end checks with relevant registries); and automated decision-making tools for calculating the amount of due benefit or PD decision outcomes.

Member States exhibit distinct variance in the digital maturity of their social security authorities' administrative systems. Currently, these can be generically grouped into three approaches:

- **Limited digital administration.** A few social security authorities reported having no digital document-handling systems or automated procedures in place to support administrative processing.
- **Partially digital administration.** In most Member States, social security institutions rely on selected digital tools to support administrative procedures; however, the processing of client requests requires significant human intervention. In many cases, this is because more mature digital administration solutions are still being developed or implemented as part of ongoing digitalisation initiatives within public administrative bodies. Among the more commonly employed digital tools are online verification tools that allow a real-time check of the validity and authenticity of PD A1, digital communication tools for more efficient and secure exchanges with clients (while still ensuring that non-digital communication remains an option, so as not to exclude certain groups – see Section 3.1) and conducting automated back-end checks with internal registries for the verification of application data or eligibility requirements. While digitising documents (including applications and supporting documents) was widely reported, not all social security bodies have advanced digital document management systems in place to centralise how electronic documents are stored, managed and tracked within the administration.
- **Advanced digital administration.** Some social security authorities have implemented advanced automation processes to support the evaluation of social benefit and PD requests. These include prefilling online application forms from registry data and implementing automated decision-making algorithms that allow caseworkers to review and approve automatically generated outcome decisions. In Finland, for example, Kela relies on various automated procedures, such as selecting only relevant questions for clients to answer when updating their personal information online based on their specific situation and, in turn, automatically modifying internal registers with new circumstances. Similarly, advanced digital administration comprises automatic termination of payments upon the receipt of a death certificate and automatic calculation of due benefits (this aspect is particularly developed within the pension benefits sector). Finally, more digitally mature administrative systems have automated notification systems for internal tracking of application status, allowing applicants to follow the stage of their application as it undergoes internal checks (e.g. this is the case for the Welfare Partners portal in Ireland).

A key finding of this study is that few social security bodies across the EU have adopted a fully automatised approach in the provision of digital social security services. In other words, in the majority of institutions and for the majority of operations, a caseworker's approval is required to finalise any automated outcome decision produced by internal algorithms (e.g.

the issuance of a PD or granting of a benefit). Such 'semi-automated procedures' are considered to be the most effective, insofar as automated verification offers speed and accuracy in processing social security claims, while human approval adds nuanced judgement and error-catching when the digital system is unable to verify certain situations (as illustrated by the case of the Portuguese 'pension on time' automated system). This creates a robust system that balances efficiency with careful review to ensure that benefits reach eligible recipients correctly.

The main gaps that remain, and which should be addressed to achieve more harmonised digital maturity across the EU with regard to social security bodies' internal digital administration, are the following:

- **Widespread implementation of digital document management systems.** Digital document management systems streamline the processing of social security benefit applications and PD requests, significantly reducing paperwork and manual handling. These systems enhance administrative efficiency by enabling quick retrieval of information, facilitating faster (or automated) decision-making and improving overall accuracy while minimising the risk of document loss or misplacement. They can also help to ensure that personal data are securely stored to prevent external attacks or information breaches (see Section 3.4).
- **Online verification tools for A1 PDs in all Member States.** To ensure the proper coordination of social security coverage for mobile workers across the EU, it is critical that all countries introduce secure, user-friendly online tools that allow inspection authorities and other concerned entities to quickly and reliably verify the validity of PD A1 forms issued by social security authorities in other countries. Many Member States have already set up such verification tools for foreign employers. These function to streamline the cross-border employment processes for employers, enabling them to confidently comply with regulations while safeguarding the social security entitlements of mobile workers. At the same time, administrative burdens on social security bodies are reduced, as they no longer need to manually process and respond to individual verification requests from employers, freeing up resources to focus on the processing and adjudication of core benefits.
- **Automated eligibility checks.** Automating back-end checks with internal databases is a key means of digitalising the verification and eligibility steps of social security requests. Such digital tools also help to minimise errors and prevent social security fraud (see Section 3.5). While social security institutions can build up internal databases from information they receive from external authorities, having interconnected registries at the national and international levels further facilitates this aspect of digital maturity, demonstrating another clear interlinkage with the maturity of digital infrastructure. The European Tracking Service on Pensions ([58]), an initiative that supports mobile workers in managing their pensions by connecting national pension-tracking services and providing an overview of pension entitlements throughout Europe, can be considered a useful initiative in this regard. The European Tracking Service on Pensions is used for the information purposes to allow insured persons to have on overview about their possible future right. The data used for the pension award and calculation is exchanged via EESSI once pension claim is submitted by the beneficiary.
- **Automated calculation of benefits and termination of payments.** Especially in the pension sector, establishing automated termination of payments as soon as the social insurance body is notified of a deceased client helps avoid overpayment, which in cross-border situations can potentially be more complex to recover. The automated calculation of social benefits can also be an accurate and useful tool for social security bodies to efficiently pay out or reclaim unduly paid benefits, although calculations should always be approved by human oversight to avoid exceptional errors.

3.3. Systems interoperability

Key findings from this section: system interoperability across Member States

Digital maturity in this dimension across the EU can overall be considered:

LOW ([59])

As required by the EU rules on social security coordination, the EESSI system ensures the exchanges of information between social security institutions across Europe, replacing paper-based communication. Cross-border interoperability of national systems outside EESSI remains limited. Nonetheless, one exemplary interoperable system is the

([58]) See https://www.findyourpension.eu/about-ets.

([59]) It is important to note that the overall assessment for this dimension is made on the basis of national-level initiatives, not considering interoperability and exchanges of data through EESSI.

European Online Information Service (EOA) in Germany, which provides a web interface for clerks in Member States to automatically obtain information on insured pensioners.

However, the vast majority of Member States have agreements in place with select Member States for **bulk data exchange**. While not interoperable systems per se, bulk data-exchange agreements support the social security institutions of countries that experience regular flows of mobile citizens in verifying high volumes of cross-border requests. Such agreements are most common in the field of pension benefits for the cross-border exchange of death certificates, which is one of the social security branches with the highest volume of cross-border requests.

The main benefits of having interoperable systems include **reducing processing times** for cross-border cases and **error and fraud reduction**. Enhancing the interoperability of national systems is challenging due to the use of legacy systems, heterogeneous data models, unaligned national legal frameworks and cybersecurity concerns, but significant efforts are being undertaken at the EU level to support Member States in this regard. These efforts include the new European interoperability framework ([60]) and the ongoing EBSI-Vector and DC4EU projects ([61]).

Effective coordination of cross-border social security and proper implementation of EU coordination rules requires robust communication between Member States' social security authorities. This enables them to accurately calculate benefits, verify the eligibility of claimants, exchange relevant data and resolve disputes for EU citizens who move between countries.

As required by Regulations (EC) 883/2004 and 987/2009, the **EESSI** system is the **main tool for data exchange** in the field of cross-border social security coordination. Itelies on a messaging system with defined processes, through which Member States send data requests to competent social security institutions in other Member States. EESSI enables legal, semantic and technical interoperability. Several Member States (e.g. Bulgaria, Ireland and Cyprus) reported that EESSI is currently sufficient to process cross-border cases in the various social security fields. As of 2024, EESSI successfully interconnects 3 350 social security institutions across the 27 Member States plus Iceland, Liechtenstein, Norway, Switzerland and the United Kingdom ([62]). An average of 3.8 million messages are sent through EESSI each month through specific business use cases, with the system having handled a total of 27 million cases of mobile citizens since 2019 ([63]).

Consequently, where EESSI is deemed to be a sufficient and adequate tool for the handling of cross-border cases, further efforts to set up data-exchange channels, going beyond the current legislative framework, might not be considered pressing. On the other hand, in some social security fields with high volumes of cross-border cases, such as pension benefits, Member States seek to set up parallel initiatives which complement EESSI system to facilitate cross-border data exchange and ensure accurate coordination of social security benefits. The assessment in this section focuses on such parallel initiatives beyond EESSI ([64]).

Information systems interoperability refers to the ability of different information systems, devices and applications to access, exchange and use data in a coordinated and standardised manner. Interoperability is 'the ability of information systems to exchange data and enable information sharing. It improves the efficiency and effectiveness of Europe-wide information-sharing tools by ensuring the technical processes, standards, and tools that allow EU information systems to work better together' ([65]).

Regulation (EC) No 883/2004 emphasises the progressive adoption of digital administration procedures by Member States for the exchange, access and processing of social security data. Electronic documents must be accepted across borders within the EU, provided secure systems are in place to prevent unauthorised access or alterations, ensuring the reliability and protection of personal data in these digital processes (see Section 3.4).

Systems interoperability is needed so that individuals can maintain their social security rights as they move across borders within the EU. Digital databases must be able to exchange data between countries and institutions seamlessly. This means leveraging a combination of technologies, standards and protocols designed for secure, efficient and compliant data sharing.

([60]) See https://ec.europa.eu/isa2/eif_en/.

([61]) See https://www.ebsi-vector.eu/en/.

([62]) In 2024, EESSI was in full production in 17 participating countries and beyond 90% of implementation in the remaining 15. The date when EESSI is expected to be in full production in all 32 participating countries is June 2025.

([63]) European Commission, 'Social security coordination – Digital information exchange system', EESSI Q3 2024 factsheet, 4 November 2024, https://ec.europa.eu/social/BlobServlet?docId=17938&langId=en.

([64]) EESSI is overseen by EU bodies (the European Commission and the Technical Committee for Data Processing) and not covered in this study.

([65]) European Commission, 'Frequently asked questions – Interoperability of EU information systems for security, border and migration management', European Commission website, 12 December 2017, https://ec.europa.eu/commission/presscorner/detail/en/MEMO_17_5241; Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act) (OJ L, 2024/903, 22.3.2024, http://data.europa.eu/eli/reg/2024/903/oj).

These include the following:

- **Application programming interfaces (APIs).** Cross-border or EU-level interoperability could technically be a relatively straightforward: it could (technically) be achieved based on APIs that would enable to request or send information directly between national systems in real time. This type of architecture is currently more of an exception than a rule. Member States engage in negotiations on bilateral agreements or rely on EESSI (because of the defined business processes). Several other reasons for this are listed in the Section 3.3.2..
- **Data protection and compliance.** Compliance with data-protection regulations such as the general data-protection regulation (GDPR) is mandatory in cross-border social security data exchange. This entails technical and organisational measures to ensure data privacy, integrity and confidentiality.
- **Secure communication.** Given the nature of social security data, secure communication protocols are crucial.
- **Common data formats and standards.** Individual Member States have national social security systems, but, for effective systems interoperability, they should adhere to standardised data-exchange formats. This is to ensure that data are universally understandable and usable across borders. Common formats such as JSON and XML enable structured data exchange and ensure that the diverse systems 'speak the same language'. The data exchange needs to follow a shared data model (e.g. EESSI).
- **Identity management.** Access to these databases requires strict identity verification to ensure that only authorised entities can access data. Member States implement authentication mechanisms to verify the identity of users accessing social security databases across borders.

Interoperability in this context explicitly ensures that disparate national systems can exchange, process and validate social security data seamlessly, realising transnational social security rights. Data-exchange layers related to interoperability can be divided into organisational, legal, semantic and technical ([66]).

- **Technical interoperability** means that IT systems and networks across Member States use compatible protocols, APIs and encryption mechanisms for data exchange.
- **Semantic interoperability** means that systems use standard vocabularies, data definitions and business logic for social security data. This ensures that data have the same meaning across Member States.
- **Organisational interoperability** means that business processes and workflows across Member States are aligned to ensure that the data exchanged triggers standardised responses (e.g. validating claims and updating contributions).
- **Legal interoperability** means ensuring that organisations operating under different legal frameworks, policies and strategies can still work together.

3.3.1. Implementation of interoperable systems for cross-border data reconciliation

A key finding emerging from this study is that **interoperability between social security authorities' digital systems for cross-border coordination outside EESSI is rare**. This can be explained by the fact that, for branches such as family benefits, EESSI is often deemed a sufficient tool for cross-border data reconciliation.

Nonetheless, some countries have reported implementing interoperable systems for social security coordination. One good example is the national European Online Information Service (EOA) in Germany, which provides a web interface for clerks in Member States to obtain information on insured pensioners in Germany. In contrast to EESSI, which mostly provides manual driven data exchanges (although some countries successfully employ automated processes and integration with national systems), this is an automatic information retrieval procedure, which issues relevant information upon request (i.e. without any involvement of clerks in Germany). The EOA started as a service between the German Pension Insurance Institute and the Italian National Social Security Institute and has since been made accessible to other states. Similarly, at the national level, in Belgium the Crossroads Bank consolidates social security information across multiple databases, and in Hungary up-to-date public records are accessed by relevant social security bodies using a central government application.

Beyond EESSI, cross-border data requests are typically carried out by social security authorities using direct secure email. One exceptional example of a digital system for cross-border requests comes from Lithuania, where the Vilnius Office of

([66]) European Commission, *European Interoperability Framework (EIF) for European Public Services*, Annex 2 to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services', COM(2010) 744 final, pp. 1–35, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52010DC0744.

the State Social Insurance Fund Board receives password-protected requests from competent social security institutions in Belgium via a secure sending tool for public services and federal organisations (Belnet FedSender) ([67]).

Therefore, data-exchange agreements consolidated by various Member States, mostly in relation to death certification data for pension benefit coordination, can be considered the main efforts undertaken at the national level for facilitating cross-border data exchange (Table 5).

One the one hand, the bulk data-exchange process is fully digitalised, facilitating timely and accurate exchanges of information on deceased pensioners between social security authorities. This ensures that records of the receiving institutions are updated promptly, preventing overpayments and maintaining accurate data. Notably, Germany has facilitated bulk death data exchange through its Secure Platform for the Exchange of Data (SPAD), which is used to exchange structured data about pensions and deaths with other states. In countries such as Hungary, data matching following bulk data exchanges is automatic, meaning that deaths are processed directly, resulting in the immediate termination of payments to prevent unduly paid benefits.

On the other hand, bulk data-exchange agreements differ from interoperable systems, as such agreements do not include common access to cross-border registers. Moreover, while these agreements can address immediate needs, they are not scalable and limit the potential for broader EU-wide interoperability. Bilateral agreements often require renegotiation or adaptation when new technologies or regulations are introduced, further complicating efforts to harmonise social security coordination.

Table 5. List of bilateral agreements for exchange of death data

Member State	Country or countries with which it has bilateral agreements for bulk exchange of death data
AT	CZ
BE	CH, DE, ES, FR, IT, LU, NL
CZ	AT, SK
DE	AT, BE, BG, CH, DK, EL, ES, FI, FR, HR, HU, IL, IT, LU, NL, PL, SE, SI, UK
DK	CH, DE, ES, FR, IS, NO, PL, SE
EE	FI, LT, LV
ES	BE, CH, DE, DK, FR, NL, PL, SE
FI	DE, EE, NO, SE
FR	BE, CH, DE, DK, ES, IT, LU, PT
HR	AT, CH, DE, PL, SI
IS	DK, SE
HU	DE
IT	AT, BE, CH, DE, FR, LU, NL, PL
LU	BE, DE, FR (IT and PT are planned)
LV	EE, LT
NL	BE, DE, DK, ES, among others
NO	DK, FI, SE
PL	CH, DE, DK, ES, HR, IT, NL
SI	DE, HR (AT and IT are planned)
SE	DE, DK, ES, FI, IS, NO, PL
SK	CZ

Source: Milieu Consulting, based on the EU survey and interviews. Information for Czechia was also obtained through consultation with the national delegation to the Technical Commission for Data Processing in February 2025.

3.3.2. Main barriers to interoperability

The main barriers that explain **low levels of advanced interoperability** across social security systems are legacy system integration, heterogeneous data models, cybersecurity and alignment of national legal frameworks.

([67]) https://belnet.be/en/services/cloud/belnet-fedsender.

Legacy systems

The term legacy systems refers to older software or hardware systems that continue to be in use despite newer technologies. These systems were often built years or even decades ago and may no longer meet current standards. Legacy systems are crucial because they hold essential historical data and are deeply embedded in national processes. These systems often manage key social security functions. Despite being outdated, they remain indispensable to ongoing operations. Ensuring that legacy systems can interoperate with new digital tools is essential for maintaining service continuity, improving efficiency and fostering cross-border collaboration.

- **Integration and architecture.** Legacy systems are not designed for modern integration and lack appropriate architecture and API support, leading to significant difficulties in cross-border and EU-wide compatibility. Most Member States do not yet have established API integrations for exchanging social security data, although several expressed an interest in pursuing this in the future (Cyprus and Norway).
- **Fragmentation.** The fragmented nature of legacy environments increases operational complexity and costs, and it hinders smooth internal and external collaboration, particularly for cross-border integration. For example, the ongoing harmonisation of systems for health insurance by the Austrian public health insurance fund, Österreichische Gesundheitskasse (ÖGK), is seen as a massive internal challenge. Fragmentation complicates efforts to standardise data formats, processing and identifiers and thus increases the difficulty of implementing cross-border digital tools and services.
- **Compliance.** Legacy systems, built for national needs, struggle with adapting to evolving data-protection regulations and EU-wide standards, creating costly compliance and integration challenges. Several countries report that negotiating cross-border agreements, especially in the pensions sector, can take years. The German EOA, for example, faced delays of three to four years in establishing agreements with foreign administrations. Adapting such systems to new regulatory demands can require costly, time-consuming overhauls or the introduction of complex workarounds, further delaying effective data exchange.
- **Outdated processes.** Legacy systems rely on outdated, manual or batch-based processes, which contribute to inefficiencies, increased costs, delays and operational risks. Unlike modern system architectures that are geared towards real-time or near-real-time processing, legacy systems often handle tasks in daily or weekly batches, creating unnecessary delays and self-inflicted operational bottlenecks. This can be particularly problematic in cross-border contexts, where real-time data exchange is crucial to be able to make timely decisions. Outdated processes not only slow down cross-border coordination but also increase operational risks, such as data mismatches, lost information or delayed service provision.
- **Maintenance.** The workarounds required to maintain legacy systems introduce new cybersecurity threats and heighten operational vulnerabilities, exposing organisations to potential risks. As these systems age, they require increasingly complex workarounds. These workarounds can create additional vulnerabilities, especially in terms of data security – a critical concern for the sensitive information managed in this area.
- **Data inconsistencies.** Legacy systems often handle inconsistent data formats and identifiers, complicating data matching and hindering integration with broader EU-wide standards. Various countries use different unique identifiers for individuals, complicating the matching of data across borders. For example, Belgium and France struggle with identity matching due to different identification numbers, while discrepancies in name conventions across countries, such as in Germany and Hungary, also hinder data alignment.

Heterogeneous data models

Heterogeneous data models are the diverse ways in which different systems and organisations structure and manage data. In the context of cross-border social security coordination, this heterogeneity presents significant challenges due to variations in data models, formats and standards.

- **Localised data models.** Countries have developed data models tailored to local needs and regulations, administrative frameworks and cultural contexts, creating challenges in cross-border data integration. One such example comes from the health insurance sector: the National Connector Software portal, in production since March 2024, facilitates the cross-border exchange of basic health data and prescription data between eight Member States (CZ, EE, ES, FR, LV, LT, PL and PT). It supports requests for and the display of patient data from other countries, as well as requests for, the viewing of and the issuing of the prescription list of a foreign patient. In Latvia, the National Connector Software portal is used by residents, doctors and pharmacists, as well as supervisory authorities and administrators, for social security coordination purposes in the field of sickness benefits. However, the different classifications of Latvia must be mapped against a classification developed by the EU, which takes time.

- **Naming variability.** Variability in data entry practices, such as differences in naming conventions, contributes to reconciliation errors and complicates data-matching efforts. For instance, in some countries, surnames are written before first names, while others follow the opposite convention. Variations in how accents, special characters and other linguistic elements are handled further exacerbate this problem, making automated data matching difficult and prone to errors. Differences in how compound names or family names are recorded in national systems have led to discrepancies when attempting to match records for social security benefits or healthcare entitlements (reported in DE, ES, LU, HU and NL).
- **Cultural differences.** Differences across administrative, cultural and linguistic frameworks further hinder the alignment of data models and cross-border collaboration. Different administrative traditions and languages can affect how data are structured, recorded and interpreted, creating barriers to the creation of interoperable systems. In countries with more decentralised administrative systems, data models may vary even between regions within the same country. Cultural differences in how data are handled also lead to variation in the interpretation of key data points, such as dates, health conditions and financial contributions.
- **Inconsistent identifiers.** Variations in identification numbers, national identifiers and key data points such as names, addresses and dates of birth across different Member States make data matching difficult across systems and borders. Member States have different local systems for assigning unique identifiers, which leads to difficulties when attempting to match data for individuals moving across borders.

The lack of harmonised data models and the reliance on bilateral agreements impede the scalability of data exchange across the entire EU. Additionally, the absence of common data models leads to manual data-matching processes, increasing the risk of human error and causing a drift in data accuracy over time. Several countries, including Italy and Luxembourg, still rely on manual or paper-based exchanges for certain social security processes. While efforts are under way to automate and integrate these systems, progress is slow, and the reliance on outdated methods continues to be a bottleneck for timely and efficient data exchange. Addressing these challenges requires the harmonisation of data standards and practices.

Cybersecurity and data protection

Cybersecurity and data protection are important for making the exchange of personal information across borders secure, especially in the realm of social security. These ensure that sensitive data, such as health records, pension information and unemployment benefits, are safeguarded against unauthorised access, breaches and misuse.

- **Diverse interpretations of regulations (especially the GDPR).** Varying interpretations of the GDPR and privacy regulations across countries hinder integration and interoperability, leading to delays and halting existing bilateral agreements. Legal concerns over privacy and data protection can limit or delay the sharing of personal information. For instance, in Belgium, privacy rules halted exchanges of employment-related data between Belgium and Germany. Similarly, the challenges surrounding accessing foreign databases are due to legal concerns, such as those identified between Belgium and France. Legal concerns over data privacy often lead to delays in implementing cross-border digital services or even halt data-sharing efforts altogether. Countries are reluctant to exchange personal data without explicit clarity on legal obligations, especially when non-compliance with the GDPR can result in significant fines and reputational damage.
- **Security requirements.** High-security requirements, often tailored to national needs, add complexity and slow down the process of achieving interoperability, counteracting EU-wide efforts. Countries such as Czechia prefer bulk data-matching solutions instead of real-time database interconnection due to security concerns. While security is of the highest importance, overly stringent national requirements that are not harmonised can obstruct progress towards interoperable solutions. This tension between ensuring security and enabling functionality is a recurring challenge.
- **Lack of standardised security protocols.** Inconsistent and non-standardised security protocols across Member States impede the development of a cohesive, secure and interoperable EU-wide data-exchange framework. The absence of common standards makes it difficult to ensure that the data exchanged across borders are consistently protected, and it slows down the process of integrating digital tools.
- **Outdated security practices.** The reliance on manual processes for security oversight, password-protected exchanges and the slow adoption of EU-wide solutions introduce inefficiencies and create additional barriers to real-time data exchange. As more modern systems are introduced, Member States must decommission these outdated practices to ensure compliance with current cybersecurity standards and to enable real-time, secure data exchange.
- **Decommissioning of legacy systems.** The decommissioning of secure legacy systems introduces new challenges, as national systems are often not ready to adopt interoperable, secure and standardised EU-wide solutions. While outdated systems need to be replaced with current and interoperable solutions, the transition period can expose vulnerabilities and create temporary new gaps in security.

The fear of data breaches and concerns over cross-border data sharing result in a reliance on less secure and slower bulk data matching and slower adoption of secure, interoperable solutions. The fear of data breaches not only slows the adoption of new technologies but also limits the types of data exchanged. As a result, only non-sensitive or aggregated data may be shared.

Unaligned national legal frameworks

Unaligned national legal frameworks complicate the seamless exchange of information and integration of services across Member States. Although the aim of EU law is not to harmonise the national social security legislations, addressing these challenges requires efforts to create a consistent legal environment that supports seamless data exchange.

- **Varying data-access restrictions.** Different national interpretations of the GDPR and varying data-access restrictions complicate cross-border data sharing and integration efforts. These differences create obstacles to integration, as countries may impose restrictions that are more stringent than required by EU law. Without a standardised approach to data access, cross-border collaboration remains fragmented, and the development of integrated digital tools is delayed.
- **Divergent legal frameworks.** A lack of harmonised social security laws and different legal standards for identification across countries create barriers to interoperability and collaboration. This makes it difficult to align systems for cross-border coordination.
- **Legal barriers to EU solutions.** National legal frameworks often impose specific requirements that complicate the adoption of EU-wide solutions. These barriers are common in areas such as pensions and healthcare, where national laws may dictate unique procedures or conditions for data sharing. These legal barriers prevent Member States from fully adopting EU-wide solutions, even when technical solutions for interoperability exist.
- **Security concerns.** Legal frameworks emphasise data security and confidentiality, which can hinder cross-border data sharing. Concerns about the legal obligations surrounding the protection of sensitive data, such as healthcare records, create delays in the development of interoperable solutions.
- **National variations.** Differences in legal definitions, requirements and administrative processes across Member States further complicate cross-border social security coordination. National variations in areas such as pensions and healthcare make it difficult to create a unified legal framework for cross-border data exchange. Efforts to standardize data exchange and make national legal frameworks compatible are often slow and are complicated by the need to balance national sovereignty with EU coordination.
- **EU-level legal harmonisation.** The lack of consistent legal standards and the time-consuming process of legal coordination highlight the urgent need for further EU-level standardisation to enable seamless data exchange. While technical solutions exist for interoperability, these cannot be fully realised without mutually compatible legal frameworks to support cross-border data exchange, which leaves cross-border social security coordination having some inherent limits.

To conclude, while technical solutions exist for interoperability, significant legal, administrative and operational barriers continue to hamper cross-border cooperation in the social security domain. Addressing these issues will require not only further standardisation and investment in technical solutions but also legal harmonisation and continuous cross-border collaboration.

3.3.3. Digital maturity assessment and areas for improvement

Interoperable and secure digital infrastructure is indispensable for data exchange between different national systems, enabling social security authorities to duly complete cross-border checks and coordinate the provision on social security benefits in accordance with Regulations (EC) No 883/2004 and No 987/2009. Digital maturity in this dimension thus ensures that citizens' social security information can be easily, promptly, accurately and safely shared across borders, facilitating timely access to benefits and reducing administrative burdens for both individuals and institutions.

Regarding the cross-border interoperability of digital systems – particularly internal registries – a more varied picture emerges. Overall, the following trends in digital maturity across Member States emerge:

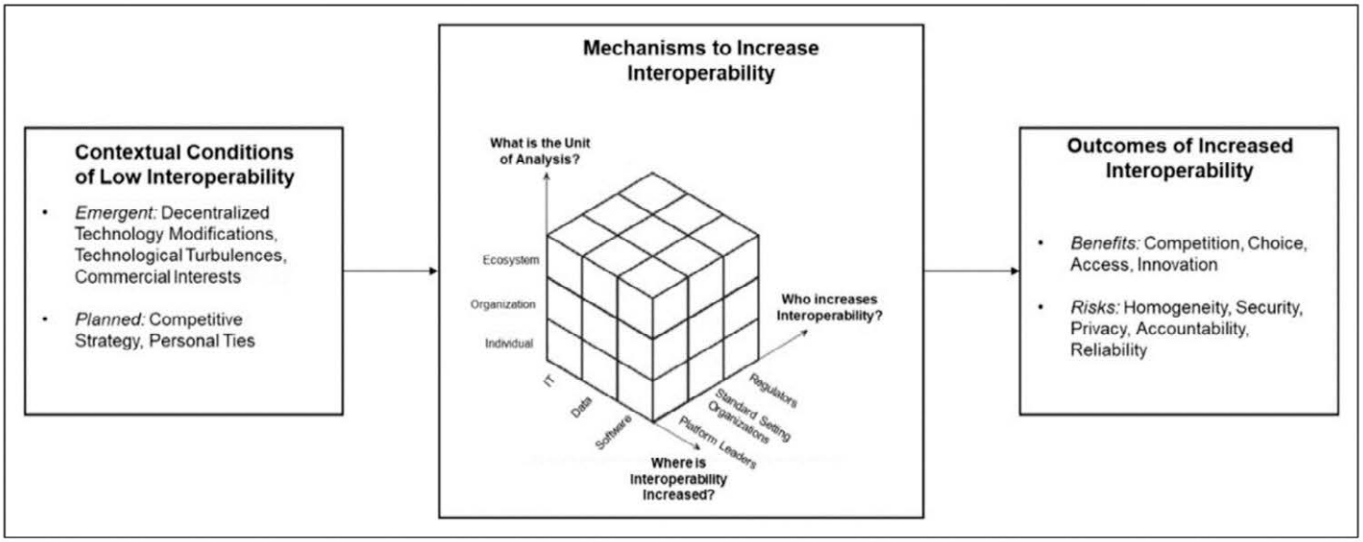
- **Reliance on EESSI.** Social security authorities in some Member States confirmed that the EESSI tool is currently sufficient in supporting cases of cross-border information exchange. No other digital tools or interconnection of databases with other countries are therefore in place. However, it is important to note that the EESSI infrastructure should be closely monitored and adapted as Member States' progress in their digitalisation efforts at the national level. For instance, one of the current workstreams of the business process improvement project under EESSI is devoted

to improving the EESSI processes and data model to accommodate the automation procedures being introduced by social security authorities. Measures include, for instance, data exchange traceability, person identification improvements, process predictability or the reduction of free-text data fields in the EESSI system design.

- **Data-exchange agreements.** Several countries have data-exchange agreements with select Member States. Such agreements are particularly common in the field of pension benefits. A data-exchange agreement in this field establishes a formal framework for countries to share death certificate information in bulk, ensuring timely updates to pension systems across borders and preventing improper payments while safeguarding sensitive personal data. A number of Member States rely on File Transfer Protocol (FTP) servers provided by the European Commission to execute bulk data exchanges. In this respect, discussions are ongoing on the options for replacing existing FTP exchanges to enhance security, data protection, and increase interoperability in the future.
- **Introduction of interoperable databases.** Interoperable databases are one of elements to allow simplified information sharing between European countries' social security systems, enabling quick verification of eligibility, accurate calculation of benefits and efficient processing of claims for mobile citizens. These systems typically comprise standardised data formats, common semantic models and secure APIs for real-time data exchange, ensuring that diverse national systems can communicate effectively despite variations in their underlying architectures. Due to several limitations, such as data privacy concerns and the difficulties of integrating different legacy systems, cross-border interoperable systems are rare. Examples include the Crossroads Bank in Belgium, which consolidates social security information across multiple databases at the national level, and the German Secure Platform for the Exchange of Data (SPAD), which is used to exchange structured data about pensions and deaths with other states. Improving national EESSI implementation and automation could be another approach towards more efficient cross-border data exchanges.

To enhance and organise efforts for greater EU-wide interoperability, the three-dimensional framework from the academic literature ([68]) shown in Figure 1 can serve as a comprehensive approach to understanding the key drivers of interoperability.

Figure 1. Three-dimensional framework for conceptualising interoperability



NB: This model has a private-sector focus.
Source: Hodap, D. and Hanelt, A., 'Interoperability in the era of digital innovation: An information systems research agenda', *Journal of Information Technology*, Vol. 37, No 4, 2022, pp. 407–427.

By applying this three-dimensional framework (focusing on the unit of analysis, where interoperability is increased and who increases interoperability), the following conclusions can be drawn on how interoperability can be increased across Member States and achieve a greater level of digital maturity in this dimension.

([68]) Hodap, D. and Hanelt, A., 'Interoperability in the era of digital innovation: An information systems research agenda', *Journal of Information Technology*, Vol. 37, No 4, 2022, pp. 407–427.

What is the unit of analysis?

- **Ecosystem.** The primary focus of the analysis is the broad cross-border social security ecosystem. The challenges outlined emphasise the need for an ecosystem-wide approach, especially when dealing with different countries' regulations and administrative processes, such as the inconsistency in social security laws across nations and different identification systems.
- **Organisation.** At the organisational level, national social security systems and administrative bodies encounter difficulties due to varying data formats, legal frameworks and security standards. The lack of standardised solutions makes inter-agency cooperation challenging.
- **Individual.** At the individual level, the analysis highlights that citizens dealing with cross-border social security issues are impacted by inefficiencies such as manual data matching, human errors and delayed exchanges. Different identification numbers and personal data standards (e.g. names and birth dates) further complicate integration.

Where is interoperability increased?

- **Software.** There is a strong emphasis on software-level challenges. Developed with unique data models, national social security systems contribute to fragmented software architectures that hinder seamless data exchange. The lack of harmonised software standards across borders has led to dependence on manual processes and non-interoperable bilateral agreements.
- **Data.** The variability in data-entry practices (naming conventions, identification numbers, etc.) and inconsistent data models are significant roadblocks for cross-border interoperability. Data-quality issues arise from mismatches in formats, identifiers and regulations. Additionally, the GDPR and privacy laws contribute to a lack of data harmonisation.
- **IT.** This report highlights the technical complexity of integrating systems across borders due to inconsistent data formats and incompatible IT infrastructure. Countries use different technologies, further complicating cross-border data-integration efforts.

Who increases interoperability?

- **Regulators.** The role of national regulators is critical in shaping the legal frameworks that affect cross-border data sharing. Different interpretations of the GDPR across countries slow down integration, creating legal barriers to adopting interoperable solutions.
- **Standard-setting organisations.** There is a noted lack of consistent standard setting across the EU. Bilateral agreements do not scale across the EU. The absence of a common legal and technical framework hinders multilateral agreements and comprehensive solutions that span the entire ecosystem.
- **Platform leaders.** In this context, platform leadership comes from national agencies or large social security platforms operating within each country. The reluctance to adopt EU-wide solutions due to legal, security and privacy concerns undermines cross-border efforts.

This analysis using the framework highlights the various dimensions of interoperability challenges in social security systems within the EU context. Joint initiatives such as EESSI and the European interoperability framework have laid some necessary building blocks for standardisation data exchange, but further technological advancements, legal standardisation and system integration are still required. Member States continue to align their technical infrastructures, regulatory frameworks and operational processes with the aim of achieving cross-border social security coordination.

3.4. Network security and data protection

Key findings from this chapter: network security across Member States

Digital maturity in this dimension across the EU can overall be considered:

HIGH

All Member States show a strong commitment to and consistent implementation of tools for ensuring high levels of data and network security, demonstrating advanced digital maturity in this dimension. This is a clear reflection of recent EU legislative efforts in this field, most notably the GDPR.

The most common strategies that are implemented by Member States to ensure high levels of network and data protection include secure authentication, secure servers, security audits and end-to-end encryption. Moreover, secure communication channels (outside EESSI) are deemed a priority by most of the Member States, with only a very limited number of social security authorities communicating with clients via (unsecure) email.

As Member States increasingly rely on digital tools and platforms to manage and share citizens' personal information, the need for robust network security becomes critical. Additionally, the sensitive nature of social security data, which often includes personal information such as health records, employment history and financial details, necessitates the highest standards of data protection. Any breach of these data could lead to severe consequences, including identity theft and fraud, underscoring the critical need for comprehensive security protocols.

Article 77 of Regulation (EC) No 883/2004 sets specific rules for the communication of personal data between authorities or institutions of Member States. Notably, the transmission of these data follows the data-protection laws of the sending Member State. Any further processing, such as storage, alteration or destruction, is governed by the data-protection laws of the receiving Member State. These rules ensure compliance with EU requirements on the protection and free movement of personal data.

Ensuring that such information is protected from unauthorised access is therefore not merely a technical requirement but a fundamental obligation to the citizens whose data are being managed. Indeed, the European declaration of digital rights and principles ([69]) highlights the importance of data protection and security in the digital transition. As a result, initiatives to further digitalise social security benefit applications and procedures must be carefully developed to ensure compliance with relevant EU and national data-protection laws.

The GDPR, in particular, is a central component of data-protection strategies across the EU. The GDPR mandates strict standards for data privacy and security, and failure to adhere to this regulation can result in significant legal and financial penalties. Similarly, the eIDAS regulation, which in addition streamlines cross-border interactions by guaranteeing mutual recognition of national eIDs, seeks to bolster trust in online services by providing a secure and reliable digital ecosystem across the EU.

However, secure and protected digital services offer other benefits beyond safeguarding personal data and compliance with legal regulations. For instance, they help build and maintain trust in digital infrastructure among Member States, which is essential for the efficient delivery of social security services. Furthermore, robust network security measures are vital in preventing cybersecurity threats that could disrupt services. As the EU continues to advance its digital transformation efforts, ensuring the protection of personal data is crucial for gaining public confidence in digital initiatives.

3.4.1. Tools for digital system security

Strict implementation of the GDPR requirements was reported by the vast majority of Member States as a central element underpinning their network- and data-security strategies. In addition, various procedures to prevent data breaches and protect the personal data of clients were reported across countries, including the following:

- **Secure authentication.** Secure authentication, which has been implemented in various forms by all Member States, refers to the process of verifying a user's identity in a way that protects their data against unauthorised access. It typically involves strong methods, such as multifactor authentication or encrypted credentials, to ensure that only legitimate users can access a system or service and perform critical actions. In this way, authentication walls protect digital systems from unauthorised access, data breaches and cyberattacks. On the client side (cross-border workers), secure authentication tools include **e-login solutions in accordance with the eIDAS regulation** and using **online identity-verification tools** or authentication tokens. On the institutional side, tools include implementing strict access controls such as **role-based access**, which seeks to limit data exposure by ensuring that only authorised personnel can access client files (CY, LU, MT, NL, AT, PL, SI (Box 18) and FI).
- **Secure network servers.** Across Member States, the network servers of bodies processing social security data are equipped with security protocols to protect stored and transmitted data from unauthorised access. For instance, firewalls act as barriers between trusted internal networks and untrusted external networks, filtering traffic to block malicious activities. On the other hand, virtual local area networks (VLANs) segment networks to isolate sensitive data,

([69]) European Commission, European declaration on digital rights and principles for the digital decade (OJ C 23, 23.1.2023, p. 1, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001).

prohibiting system access from public networks, reducing the risk of potential attacks and enhancing overall network security. Additionally, in Slovakia, geo-blocking of access from risky countries has been applied.

- **Certification and audits.** Adhering to security standards and conducting regular audits provide a structured framework for risk and vulnerability assessments, implementing effective security controls, and continuously monitoring and improving security practices to safeguard sensitive information. For instance, International Organization for Standardization (ISO)-classified security standards (e.g. ISO 27001) have been implemented by social security institutions in Croatia, Lithuania, Poland and Finland. In Germany, the Pension Insurance Institute's IT infrastructure, services, processes and internal guidelines are regularly audited against information security standards set out by the German Federal Office for Information Security. Several Member States implement regular security audits to ensure that safety requirements and standards are met.
- **Data-protection officers.** The GDPR requires all public authorities that process personal data to appoint a data-protection officer to ensure compliance with legal requirements. In some social security institutions (e.g. BE, CZ, IT, LT, HU and FI), specially trained data-protection officers are integral to the data-protection strategy. They not only oversee proper implementation of relevant data-protection requirements, but also conduct security audits and provide consulting support to further strengthen overall system safety.
- **Incident response plans.** A well-defined incident response plan outlines the steps to take in the case of a network- or data-security breach, facilitating the timely resolution of information security incidents. Several Member States reported having clear procedures in place to efficiently manage and limit security incidents. For instance, in France, most security incidents relating to unemployment benefits within the national employment agency France Travail come from external contractors. Thus, a chain of command is in place to notify any leak to the data-protection authority within 48 hours ([70]).

Box 18. Good practice: data-protection measures of the ZPIZ in Slovenia

When delivering cross-border (and domestic) social security services, the ZPIZ prioritises the protection of personal data according to the GDPR, national law and internal regulation requirements through a robust framework of technical and organisational measures.

Technical measures include the following:

- **Secure infrastructure.** The ZPIZ maintains a robust IT infrastructure with robust security protocols and systems to safeguard data confidentiality and integrity.
- **Access controls.** Stringent access controls restrict access to personal data on a need-to-know basis. Only authorised personnel can access data for specific processing tasks.
- **Write-once, ready-many (WORM) technology.** Documents are written only once in the document system and cannot be edited. Any alterations to the document by the user produce a new version of the document but keep the previous version.
- **Digital signatures.** The ZPIZ uses digital signatures to verify the authenticity and origin of electronic documents. Any alteration attempt would invalidate the signature, alerting the ZPIZ to potential tampering.
- **Audit trails.** Comprehensive audit trails track all document activity, recording any access, modification or deletion attempts. This detailed record provides accountability and helps detect suspicious activity.
- **Regular backups.** The ZPIZ maintains regular backups of electronic documents to a secure off-site location. This ensures data recovery in the case of incidents such as hardware failures or cyberattacks.

Organisational measures include the following:

- **Training and awareness.** The ZPIZ conducts training programmes for staff to ensure that they understand their data-protection responsibilities, they implement best practices for handling personal data and they are equipped to handle electronic documents responsibly.
- **Data-processing agreements.** The ZPIZ establishes formal data-processing agreements with partner institutions in other states. These agreements clearly specify roles, responsibilities and data-security requirements for cross-border data exchange.
- **Security policies.** The ZPIZ has implemented clear and documented security policies that set out rules on user behaviour and best practices for handling electronic documents.

([70]) Interview with France Travail (23 July 2024).

- **Cross-border social security.** The ZPIZ's data-protection measures are comprehensive and apply equally to both domestic and cross-border social security data-processing activities.
- **Incident management.** Documented procedures guide the reporting and timely resolution of information security incidents and vulnerabilities within the ZPIZ's systems.

3.4.2. Ensuring secure communication channels for social security data coordination

Social security authorities from different Member States need to exchange data when handling social benefit requests from cross-border workers and citizens to ensure accurate calculation of entitlements, prevent fraud and verify compliance with the applicable national regulations and EU coordination rules. Some institutions use secure communication channels beyond EESSI to exchange and coordinate social security data across borders when evaluating requests for social security benefits. For instance, the German Pension Insurance Institute conducts all pension-related communication via the European Commission's Trans European Services for Telematics between Administrations (TESTA)-next generation network ([71]). Moreover, in Luxembourg, the AWOD branch prioritises digital channels with traceable records over phone communication to reduce the risk of miscommunication and maintain transparency. Blind trust is avoided, as all data exchanges and access are carefully logged and monitored to ensure accountability. Otherwise, Member States' authorities mostly reported using secure mail to coordinate information exchange across borders.

The vast majority of social security bodies reported using encryption and anonymity measures, most notably through **secure email**, to implement secure communication channels and protect sensitive personal data when being transmitted across systems. Secure email is a method of transmitting email messages that ensures confidentiality and authenticity to protect information from unauthorised access or tampering during transmission. **End-to-end encryption**, which is a key feature of secure email, ensures that only the sender and the recipient of a message can access its contents during its transmission, preventing interception by third parties, including service providers. When combined with **anonymity**, where users' identities are protected or concealed, this creates a robust layer of data security by safeguarding both the content of the communication and the identity credentials of the personal data, significantly reducing the risk of unauthorised access or tracking.

Importantly, **institutional differences** exist **even within the same country**. For instance, in France, no particular cross-country communication channels have been implemented at the moment, other than EESSI for unemployment benefit coordination by the national employment agency France Travail. In the case of need, most documents are shared with other national authorities through informal electronic communications, based on administrative cooperation. Currently, there is a pending initiative that France would like to continue developing with Belgium to share information and documents more directly, but the project has been put on hold due to difficulties in identifying the right contact people. On the other hand, CAF makes use of an integrated system to simplify the digital communication of documents and information on beneficiaries' rights with Luxembourgish authorities. However, Luxembourg is the only country with which France has such digital communication in place. With all other Member States, except for EESSI, the exchange of documents occurs by paper.

Regarding communication with clients, the vast majority of social security authorities reported implementing and favouring digital communication with clients (including cross-border workers). However, ensuring the security of digital channels remains a priority. In several Member States, **communications that contain personal data are not sent to clients via unsecure email**. For example, in Austria, ÖGK clients can send requests via email, the app or through the online website. For replies, however, the ÖGK needs to resort to letters via the national postal service to ensure data protection, as email without a digital signature is not a data-secure communication tool.

The issue of clients sending sensitive data through unsecure email was raised across multiple countries as a key risk in terms of data security. For this reason, some Member States encourage the use of more secure alternative solutions, such as the **personal data box** in Czechia and Denmark, which enables citizens to securely send electronic documents to public authorities free of charge. Other social security institutions have set up, or are currently developing, online communication services with clients that help guarantee secure communication. Where secure forms of electronic communication can be guaranteed, some institutions have removed paper communication with clients entirely (e.g. the Finnish Workers' Compensation Center for AWOD benefits). However, the majority of Member States do not discriminate against paper communication options, which continue to be offered as alternatives to digital solutions.

([71]) See https://ec.europa.eu/isa2/solutions/testa_en/.

3.4.3. Digital maturity assessment and areas for improvement

Overall, all Member States have demonstrated a **strong commitment to and significant implementation of tools to ensure high levels of data and network security**, demonstrating relatively advanced digital maturity in this dimension. This is a clear reflection of recent EU legislative efforts in this field, most notably the GDPR. Member States all reported having strategies in place to ensure high levels of network and data protection, such as secure authentication, secure servers, security audits and end-to-end encryption. Moreover, secure communication channels (outside EESSI) are deemed a priority by most Member States, with only a select number communicating with clients via (unsecure) email.

3.5. Error and fraud detection

Key findings from this chapter: error and fraud detection across Member States

Digital maturity in this dimension across the EU can overall be considered:

PARTIAL

Most Member States consider their verification systems for handling cross-border cases to be effective. Although fraud and error do not appear to be common issues for social security authorities dealing with cross-border requests, there is significant variance in Member States' implementation of specific digital tools for detection and prevention.

Most institutions with digitalised services have passive forms of fraud- and error-detection tools built into their service structure and administrative procedures (e.g. back-end checks with internal registries or cross-border data or allowing users to update their personal data online). However, active tools are less common.

Several institutions reported having no specific tools in place to target the detection of errors or social security fraud in cross-border cases, leaving room for development. Other countries have advanced significantly by utilising AI to implement data-mining and machine-learning tools as part of their fraud- and error-detection strategies. One key practice is, for example, online tools to verify the validity of PDs.

The main obstacles reported in this field are ensuring compliance with the GDPR, the limited effectiveness of digital tools that still require human assessment and the limited development of tools specifically designed for cross-border cases.

While the coordinating regulations (i.e. Regulations (EC) No 883/2004 and No 987/2009) make little reference to fraud and error, these issues have been extensively discussed in a number of reports by the European Commission in recent years ([72]). These documents highlight that fraudulent and erroneous situations can hinder the free movement of people, one of the core principles of the single market, and can have a negative impact on cross-border social security systems. For instance, errors or fraud can lead to the undue payment of benefits or cause delays and complications in processing legitimate claims, undermining individuals' rights and creating administrative burdens for authorities.

The implementation of electronic and digital solutions offers a promising approach to reducing the risk of error and fraud in cross-border social security coordination, as recognised by the European Commission itself ([73]). Digital solutions can enhance accuracy and improve fraud-detection patterns, for instance by facilitating the updating of personal information (see Section 3.1) or by automating verification procedures (see Section 3.2).

3.5.1. Detection of fraud and error in cross-border social security cases

Errors in cross-border social security can manifest in various ways. One common type involves **incorrect information updates**, as discussed in Section 3.1. For example, inaccurate address details can result in the EHIC or other PDs not being delivered or even being delivered to the wrong address, an issue highlighted by CAK in the Netherlands. Second, **wrong spelling** or differences in the spelling of the same name can result in several unintended consequences. For instance, the Norwegian Labour and Welfare Administration reports that spelling mistakes can lead to the creation of multiple personal

([72]) European Commission: Directorate-General for Employment, Social Affairs and Inclusion, *Fraud and error in the field of EU social security coordination – Reference year 2022*, Brussels, 2024, https://ec.europa.eu/social/BlobServlet?docId=27421&langId=en.

([73]) The 2024 report on fraud and error argues that the use of an electronic system can avoid human error and external interference, when it comes to intranational and international cooperation and data exchange (p. 15 in European Commission: Directorate-General for Employment, Social Affairs and Inclusion, Fraud and error in the field of EU social security coordination – Reference year 2022, Brussels, 2024, https://ec.europa.eu/social/BlobServlet?docId=27421&langId=en).

IDs, which can then make the application for documents or benefits more burdensome. In addition, the Pension Payment Directorate of the Hungarian State Treasury reports that an issue regarding the exchange of death certificates with Germany is that the spelling of names and places might change from one language to another. Such mistakes might lead to the supply of unduly paid pension benefits.

Fraud in cross-border social security can equally take various forms. An example can be the **collection of pension benefits on behalf of a deceased person** whose death has not yet been registered. The Norwegian institution in charge of pension benefits observed that such a fraud was widespread before the introduction of life certificates and the electronic exchange of death certificates in the early 2000s. Other frequently identified forms of fraud relate to forms of **fake posting** and **bogus self-employment** ([74]). Finally, **identity theft** can lead fraudsters to claim social security benefits on behalf of their victims.

Many Member States utilise **digital and automated tools for fraud and error detection**, finding them to be **effective and yielding significant results**. This is, for instance, the case for Denmark, Lithuania, Luxembourg and Slovakia. Additionally, the Belgian National Social Security Office has observed an increase in the effectiveness of its AI-based system in detecting fraud – with accelerated recovery and more cases of fraud detected – as well as a more efficient optimisation of internal processes ([75]). Luxembourg has observed a significant decrease in errors with the implementation of an automated system. Hungary noted that the automated death data exchange system has significantly reduced overpayments.

On the other hand, some countries' institutions report having limited or no digital tools in place for detecting errors and fraud (including CZ, EL, FR, PT and SE). The reasons behind the lack of digital error- and fraud-detection tools include the lack of digitisation of certain benefit fields and the lack of the necessary infrastructure.

3.5.2. Digital tools/strategies for preventing error and fraud

Over time, social organisation institutions have developed new tools to minimise the risk of error and fraud in cross-border contexts. Most forms of anti-error and anti-fraud tools are specific to single organisations, rather than to social security domains. Indeed, there is remarkable variation in the sophistication reached by different institutions.

Several institutions across different social security domains use **automated checks** to verify the correctness of information supplied by users in application processes (AT, BE, CZ, DE, DK, HR, IT, LT, LU, NL, NO, PL, SE and SK). Automated checks encompass different technologies and processes:

- **Data matching.** The majority of institutions using automated checks match the information contained in applications with information and data contained in public databases or registries. However, **only in one case are data matched with the database of another country outside the realm of life and death certificates**. This is the case of Finland, where pension data are cross-referenced with earnings-related pension and population registries and compared with those of Estonia ([76]). Where there are no interoperable databases, Member States rely on bulk data exchanges and EESSI for data matching. For instance, in Belgium, PD U1 and PD S1 authentication can be conducted only through the EESSI system by verification of the data contained in these documents via respective EESSI use cases. Automated checks are in place within the back-end systems to verify the authenticity of documents such as the S1, allowing institutions to confirm legitimacy without requiring the physical document. These checks can be conducted by various entities, including inspectors, although not exclusively.
- **Algorithms and other advanced tools (data mining, AI and machine learning).** A good number of institutions employ quite sophisticated algorithms when carrying out error and fraud detection. This is the case of Belgium, Croatia, Denmark, Iceland, Italy, the Netherlands and Slovakia. The instruments used include data mining (Denmark

([74]) De Wispelaere, F., De Smedt, L. and Pacolet, J. *Posted Workers in the European Union – Facts and figures*, Posting.Stat project VS/2020/0499, HIVA-KU Leuven, Leuven, 2022; reported through stakeholder interviews.

([75]) RSZ, *De RSZ: Geld, gegevens en sociale zekerheid*, Brussels, 2020, https://news.belgium.be/sites/default/files/news-items/attachments/2020-02/dossierPresse_170220_nl_v4.pdf.

([76]) This practice is also noted by the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the digitalisation of social security coordination: facilitating free movement in the single market, COM(2023) 501 final of 6 September 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A501%3AFIN.

and Italy ([77]), AI (Belgium ([78]) and Italy ([79]) and plausibility checks (Czechia, Germany and the Netherlands) to identify unusual patterns or behaviours indicative of fraud.

- **Other tools and processes.** A few institutions employ other methods when carrying out automated checks, such as conducting **information retrieval processes** through the use of error-detection instruments (e.g. in Austria for health insurance) or the implementation of a **data warehouse and business intelligence system** (in Luxembourg for AWOD benefits), which sends applications to clerks for reviews, allowing the identification of potential anomalies.

Automated checks always involve **some form of human intervention**. The following is a classification of countries based on their level of human intervention in automated checks:

- **Minimal human intervention.** Several institutions resort to human intervention only when automated checks have flagged certain anomalies. This is the case of organisations in Denmark (Box 19), Germany, Luxembourg, Norway, Poland and Slovakia. This approach is in line with the 'human in the loop' principle, now enshrined in the EU's AI Act (see Section 3.2.2).
- **More substantial human intervention.** A number of organisations also rely on human intervention to deal with complex situations. This is the case of institutions in Belgium, the Netherlands and Finland. For example, the security operations centre of the Dutch Employee Insurance Agency plays an active role in monitoring potential anomalies and security risks. By contrast, Kela in Finland reports that manual processing is significantly higher in cross-border cases than in domestic cases.
- **Full human intervention.** Some organisations still rely on full human intervention to detect cases of error and fraud. This is the case of institutions in Estonia, Greece, France and Malta.

Box 19. Good practice: integrated error detection with data mining and manual oversight in Denmark

Udbetaling Danmark, an institution in charge of payments across various social security domains, employs a comprehensive system that combines **automated checks, data mining and manual review to detect errors and fraud in social security applications**.

The system uses **algorithms** to analyse behaviour and transaction patterns, identifying suspicious activities such as unreported income while receiving benefits. Once flagged, these cases are reviewed by a caseworker who conducts further investigation, ensuring a balance between automated efficiency and human oversight.

The key features of the system are:

- **data mining and algorithms** – automated tools analyse data to detect patterns indicative of fraud;
- **four-eye checks and quality control** – for high-risk transactions, manual checks are performed to ensure accuracy;
- **monthly quality-control reviews** – regular evaluations ensure that the system meets a high standard of error-free cases, aiming for 97 % accuracy.

It is an effective system because of the following features:

- the integration of automated and manual processes provides a **robust** mechanism to address fraudulent activities while **maintaining the accuracy** of application processing;
- the combination of data mining and human review helps **continuously refine detection algorithms**, improving overall effectiveness.

([77]) This information is not based on the interviews but on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the digitalisation of social security coordination: facilitating free movement in the single market, COM(2023) 501 final of 6 September 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A501%3AFIN.

([78]) This is the case of the National Office of Social Security, which has implemented algorithms based on AI to combat social fraud. These algorithms read big data to understand potential fraudulent patterns. For further information, see RSZ, *De RSZ: Geld, gegevens en sociale zekerheid*, Brussels, 2020, https://news.belgium.be/sites/default/files/news-items/attachments/2020-02/dossierPresse_170220_nl_v4.pdf.

([79]) This information is not based on the interviews but on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the digitalisation of social security coordination: facilitating free movement in the single market, COM(2023) 501 final of 6 September 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A501%3AFIN.

Some countries also rely on **preventive measures** to ensure that the risk of errors and fraud is minimised upfront. The preventive measures reported include the following:

- **Automated procedures for issuing PDs (including eligibility checks and document-verification tools).** Several countries have implemented automated verification of eligibility criteria as part of PD request procedures, especially A1 PDs. For instance, in Ireland and Lithuania, the system does not allow requests for A1 PDs to be completed if the automatic data matching with internal registries is unsuccessful (e.g. if an A1 certificate has already been issued for the same period or if an employer is not registered). In the Netherlands, once the identity is checked, the system will always allow the citizen to request for a PD A1. However, if data of employment do not match internal registries, the application will not be processed automatically, but an extra manual check will be required.
- **Other countries have introduced automated online tools for employers to verify the validity of an issued PD**. For instance, in Portugal, the document to determine applicable legislation allows caseworkers to verify the authenticity of A1 documents by inserting a verification code contained in the document (Box 20) ([80]). Similarly, in Croatia (pensions) and Slovenia (pensions), the electronic documents issued have a specific QR code that allows users to verify authenticity via the link provided. Such validation tools are crucial to protect digitally issued documents against forgery, thereby preventing and facilitating the detection of social security fraud.
- **Portals to easily update personal information.** Facilitating information updates through digital solutions represents a way to reduce the risk of errors. Countries such as Denmark, Germany, France, Luxembourg, Malta and Finland have implemented this type of solution for different social security domains (see Section 3.1.1 for further information).
- **Implementation of robust identification tools.** Several countries have implemented electronic identification systems, as mentioned in previous sections. In Austria, ÖGK is noted for its use of the EU Digital Identity Wallet, which represents a harmonised solution for identification, authentication and application for social security entitlements. The Finnish Centre for Pensions currently permits only users in possession of a Finnish ID to apply electronically for A1 PDs.
- **Implementation of user-friendly portals.** For instance, the Finnish portal for earnings-related pension benefits guides users in entering data in a smooth way. Similarly, on the Hungarian website for the application of social security benefits, a personalised administration interface guides the application submission process. Moreover, the forms needed to apply for benefits contain targeted questions to allow users to better understand the process.
- **Exchange of life and death certificates.** The timely provision of life and death certificates is crucial to avoid underpayment or overpayment of pension benefits. Several countries have digitalised the provision or the cross-border exchange of life certificates, such as Czechia, Denmark, Spain, Croatia and Hungary. Furthermore, for death certificates, some forms of digitalisation and cross-border exchange exist across countries, for example in Croatia, Italy, Hungary and Finland (see Section 3.3).
- **Staff training.** Staff training is present in Hungary, to keep clerks' IT knowledge up to date, and in Lithuania and Belgium, where cybersecurity courses/trainings are provided for employees.

Box 20. Good practice: the document to determine applicable legislation used as a tool to prevent fraud in Portugal ([81])

The Portuguese Social Security Institute's recently developed **determination of legislation applicable (DLA) application** streamlines the application for the issuance of A1 PDs in Member States, Switzerland and the United Kingdom, simplifying and decreasing the length of the procedure and the time it takes to issue the documents. Through its authenticating features (e.g. a PD A1 validation tool), it **supports authorities** by ensuring a better application of the legislation and more effective prevention of errors and fraud. This tool was awarded by ELA for its innovative approach in tackling fraud.

How it works

([80]) The Institute of Social Security of Portugal was awarded for its innovative approach to combat fraud. For further information, see ELA, 'Institute of Social Security Portugal awarded for its innovative tool preventing social security fraud', ELA website, 11 July 2024, https://www.ela.europa.eu/en/news/institute-social-security-portugal-awarded-its-innovative-tool-preventing-social-security.

([81]) The following description is based on the following two sources: ELA, 'Institute of Social Security Portugal awarded for its innovative tool preventing social security fraud', ELA website, 11 July 2024, https://www.ela.europa.eu/en/news/institute-social-security-portugal-awarded-its-innovative-tool-preventing-social-security; ELA, 'Good practice: DLA application for the posting of workers – Portugal', 2024, https://www.ela.europa.eu/sites/default/files/2024-04/PT_good-practice_dla-application_posting-of-workers.pdf.

Employers, self-employed workers and clerks of can access the DLA application on the website of the Portuguese Social Security Institute and through the central social security service application. Employers and self-employed workers can **apply for PD A1 online**, and they can also **consult the status of their request**, cancel it or extend the posting.

The information provided is checked vis-à-vis the data already contained in the social security database and, if the applicant meets the requirements, the request is **automatically validated**. If the request is valid, PD A1 is sent to the employer or the self-employed worker.

Inspectors from other countries can **check potential instances of fraud** by going on the website of the Portuguese Social Security Institute and using a validation tool, which allows the authenticity of A1 PDs to be verified using a **validation code** issued by the Portuguese Social Security Institute.

3.5.3. Challenges for fraud and error detection under digitalisation

Despite the overall positive experience reported regarding the digitalisation of anti-error and anti-fraud tools, some challenges were identified:

- **Limited effectiveness of automated checks.** In Germany, the automated fraud management system for unemployment benefits functions primarily as a deterrent rather than a robust prevention tool, with its effectiveness constrained by limited follow-up on prosecutions and clarifications. In France, the data-mining system used to detect fraud as regards family benefits is not able to distinguish between minor and major instances of fraud.
- **Limited cross-border fraud-detection mechanisms.** Some countries, such as Denmark, France and Finland, reportedly lack specific digital tools for detecting or preventing fraud in cross-border situations.
- **Compliance with the GDPR.** Several countries highlight challenges related to the GDPR and privacy requirements. For example, in Belgium, challenges arise due to the GDPR and proportionality concerns, which limit the extent to which data can be automatically checked and shared. In the Netherlands, the Employee Insurance Agency highlights the need for a balance between the effectiveness of anti-fraud tools and privacy concerns as an ongoing challenge.
- **Interoperability of databases.** According to the Finnish Centre for Pensions, stronger interoperability across systems in Europe with automated data matching could improve the likelihood of error detection.

3.5.4. Digital maturity assessment and areas for improvement

Digitalisation can help to reduce and prevent error and fraud in social security coordination. This is particularly evident from the strong interconnections between error and fraud detection and all other dimensions of digital maturity. First, accessible user services allow individuals to keep their personal information up to date and to securely authenticate their identities when using online services, forming a crucial first line of defence against administrative errors and identity theft. Second, digital administration streamlines internal processes, integrating automated checks that enhance accuracy in eligibility determinations and data verification while simultaneously enabling staff to focus on complex cross-border cases. Finally, interoperable systems facilitate rapid and precise data matching across borders, while robust digital infrastructure and data security measures safeguard against external threats, creating a comprehensive approach to maintaining integrity across digital operations. Therefore, achieving high scores on digital maturity across these dimensions marks an intrinsic advancement of digital maturity with regard to error and fraud detection.

Moreover, digital tools, such as data-mining algorithms, can be used to detect errors and fraud. Member States can therefore broadly be divided into two groups:

- **Ambient digital framework for fraud and error detection.** The vast majority of social security bodies with digital administration procedures have some inherent form of error detection, such as back-end checks as part of eligibility checks with internal registries or interoperable foreign databases (posting notifications via EESSI to conduct cross-border data verification is often cited in this regard). Insofar as these digital tools are primarily designed to execute other functions pertaining to the processing of social security requests, they might be considered more passive tools for error and fraud prevention. However, many institutions across Member States reported having no specific tools in place to target the detection of error or social security fraud, leaving room for development.

- **Active digital tools for fraud and error detection.** Several Member States have developed specific digital tools for active prevention and detection of fraud and errors, demonstrating advanced digital maturity in this dimension. In Portugal, for instance, a specific application for determining applicable legislation for posted workers through a single, automatised system was developed to combat fraud related to the falsification of A1 PDs ([82]). In other countries, algorithms have been developed for fraud prevention in specific branches of social security, for instance , detecting data patterns indicative of fraud in the field of pension benefits in Denmark.

The implementation of dedicated digital error- and fraud-detection tools is an important step in achieving full digital maturity in social security coordination systems. To exploit technology's full potential in efficiently and accurately detecting error and fraud, social security bodies working with cross-border partners should focus on sharing the development of algorithms and other best practices within their field, thereby jointly developing up-to-date strategies to respond to ongoing challenges and potential new vulnerabilities of digital systems. However, the sharing of algorithm-based tools between Member States should carefully adhere to EU data-protection rules. A standard, multilateral approach to error and fraud detection will increase the overall capacity of Member States to combat social fraud and ensure smooth and proper implementation of social security coordination requirements.

([82]) ELA, ''Institute of Social Security Portugal awarded for its innovative tool preventing social security fraud', ELA website, 11 July 2024, https://www.ela.europa.eu/en/news/institute-social-security-portugal-awarded-its-innovative-tool-preventing-social-security.

4. Assessment of digital maturity in Member States

Key findings from this chapter: assessment of digital maturity in Member States

The DMA scoring of the 30 Member States reveals significant diversity across social security branches, DMA dimensions and countries.

Applicable legislation and pensions are among the most advanced branches, especially in terms of user accessibility and digital administration. In particular, **the pension domain also stands out in the systems interoperability dimension**, due to the presence of various bilateral exchange agreements on life and death information. On the other hand, social security fields such as sickness benefits in kind and AWOD appear less mature, notably in terms of systems interoperability and error and fraud detection. The low scoring in interoperability might be due to the highly sensitive and personal data involved in these two domains, which could explain the reluctance of social security institutions in sharing them.

Systems interoperability appears to be one of the least mature dimensions overall, in line with the lack of interconnection and data exchange initiatives beyond EESSI between countries ([83]). The exception is the pension domain, as mentioned above.

Among the Member States, the most advanced are Czechia, Finland, Latvia, Lithuania, the Netherlands, Norway and Sweden, which display the greatest number of digitally mature cross-border social security services. All these countries are particularly advanced in the applicable legislation and pension domains. Notably, the Netherlands and Finland also display a significant maturity level in the realm of family benefits, while Czechia is particularly advanced in the sickness benefits in cash domain. Other countries, such as Belgium, Germany, Italy, Malta and Austria, show intermediate maturity, with Belgium being particularly advanced in the pension field, and Italy being most advanced in the applicable legislation field.. Instead, other countries, such as Bulgaria, Greece, Portugal and Romania, are characterised by the lowest maturity in the sample. It is worth noting that, in some countries, there was insufficient information available to perform the scoring.

Digitalisation efforts in cross-border social security (beyond those required by EU legislation, such as the SDGR) are primarily driven by institutions' needs, resulting in varied levels of digital maturity across countries and social security branches. Pension services, for example, exhibit a high degree of digital maturity due to their widespread use and high degree of cross-border relevance. Moreover, Member States with higher numbers of cross-border workers have greater incentives to digitalise cross-border coordination and request procedures.

Importantly, advancing digital maturity brings numerous benefits to social security institutions, in addition to simplifying citizens' uptake of their social entitlements. Notably, **digitalisation enhances operational efficiency, accuracy and cross-border collaboration by streamlining processes, reducing resource needs, improving data matching to minimise errors and enabling seamless data sharing for better-informed and more secure decision-making across borders**. On the other hand, the complexity of cross-border cases makes effective digital tools particularly challenging to develop and implement.

4.1. Digital maturity assessment scores

The scoring of the 30 Member States demonstrates the wide array of digital maturity across different countries and the different social security branches (Table 6).

The countries displaying **the most digitally mature cross-border social security services are Czechia, Finland, Latvia, Lithuania, the Netherlands, Norway and Sweden**. These countries score remarkably well in the applicable legislation and pension domains in particular. Some of them are also leading in other social security sectors, such as sickness benefits in cash (Czechia) and family benefits (the Netherlands and Finland). Several countries display an intermediate maturity level

([83]) It is important to note that the assessments under this study do not cover exchanges through EESSI, but focus on parallel national-level initiatives. EESSI is overseen by EU bodies (the European Commission and the Technical Committee for Data Processing) and is subject to evaluations in this context.

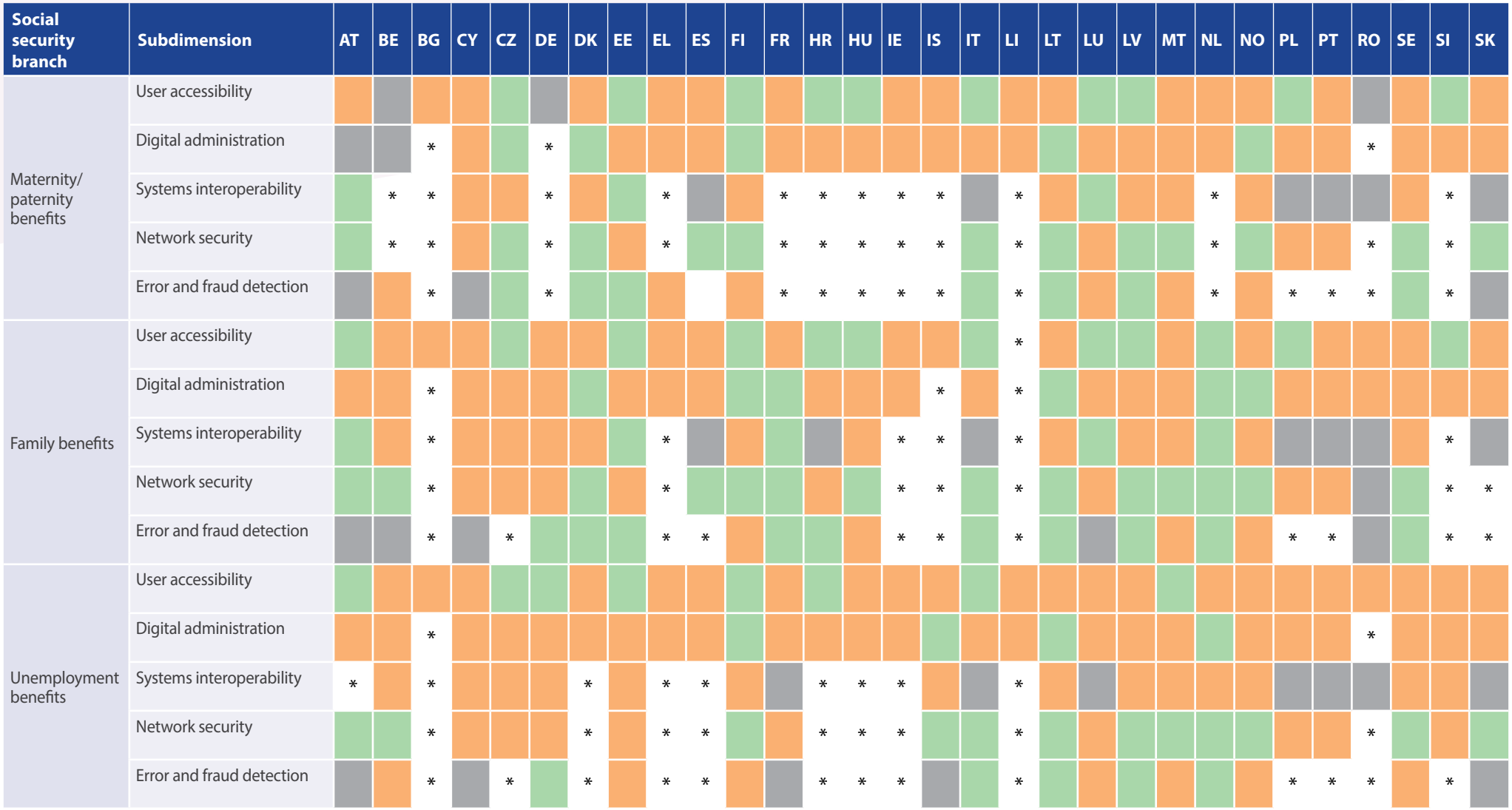
in their digital services. This is the case, for instance, of Belgium, Germany, Estonia, Italy, Austria and Slovakia. It is worth noting that some of these countries score well in certain social security domains. For example, Belgium is highly mature in the pension domain, with an advanced score in all of the dimensions in this domain. Estonia and Slovakia display a high degree of maturity in the applicable legislation domain, with an advanced score in four dimensions out of five. By contrast, countries such as Bulgaria, Greece, Portugal and Romania are characterised by the lowest maturity in the sample. It must be noted that, in certain cases, the level of unavailable information needed to perform the scoring was particularly high, such as in Bulgaria and Liechtenstein.

Among the social security domains, **applicable legislation and pension benefits** are the most digitally mature, particularly in user accessibility and digital administration, with pensions also excelling in systems interoperability. The strong cross-border dimension of these fields, such as PD A1 certifications for cross-border work and life and death certificate exchanges for pensions, might be driving their digitalisation. This exposure to error and fraud risks further necessitates advanced systems. Additionally, the high demand for pension services, influenced by population ageing, might have prompted investment in more accessible and efficient digital solutions by social security institutions.

Finally, among the dimensions, the most digitally mature are **user accessibility, network security, and error and fraud detection**. By contrast, systems interoperability displays the lowest level of maturity. An explanation of this likely lies in the strong use of EESSI reported by various social security institutions interviewed, which makes the implementation of other data exchanges and interconnected systems unnecessary.

Table 6. DMA scoring by Member State and social security branch

Social security branch	Subdimension	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK
Applicable legislation	User accessibility																		*												
	Digital administration																				*										
	Systems interoperability			*						*			*		*				*		*									*	
	Network security			*						*			*		*				*		*						*		*		
	Error and fraud detection			*						*			*		*				*		*						*		*		
Sickness benefits in kind	User accessibility																														
	Digital administration						*												*												
	Systems interoperability		*				*			*			*	*	*			*	*												*
	Network security					*	*			*			*	*	*			*	*									*			*
	Error and fraud detection		*			*	*			*	*		*	*	*			*	*								*	*		*	*
Sickness benefits in cash	User accessibility													*					*												
	Digital administration			*			*							*					*									*			
	Systems interoperability		*	*			*	*		*			*	*		*			*											*	
	Network security			*			*	*		*			*	*		*			*									*		*	
	Error and fraud detection			*			*	*					*	*		*			*						*	*	*	*		*	


Social security branch
Subdimension
AT BE BG CY CZ DE DK EE EL ES FI FR HR HU IE IS IT LI LT LU LV MT NL NO PL PT RO SE SI SK
Maternity/ paternity benefits
User accessibility
Digital administration
Systems interoperability
Network security
Error and fraud detection
Family benefits
User accessibility
Digital administration
Systems interoperability
Network security
Error and fraud detection
Unemployment benefits
User accessibility
Digital administration
Systems interoperability
Network security
Error and fraud detection

Social security branch	Subdimension	AT	BE	BG	CY	CZ	DE	DK	EE	EL	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT	LU	LV	MT	NL	NO	PL	PT	RO	SE	SI	SK
Pensions	User accessibility																														
	Digital administration			*																											
	Systems interoperability	*		*						*						*			*	*											
	Network security			*						*			*			*			*	*								*		*	
	Error and fraud detection			*		*					*					*			*	*							*	*			
AWOD	User accessibility																														
	Digital administration						*						*														*		*		
	Systems interoperability	*					*	*	*	*			*	*	*	*	*	*	*								*			*	
	Network security						*	*	*	*			*	*	*	*	*	*	*								*	*		*	
	Error and fraud detection					*	*	*	*		*		*	*	*	*	*	*	*							*	*	*		*	

Source: Milieu Consulting.

* Missing information

Low digital maturity

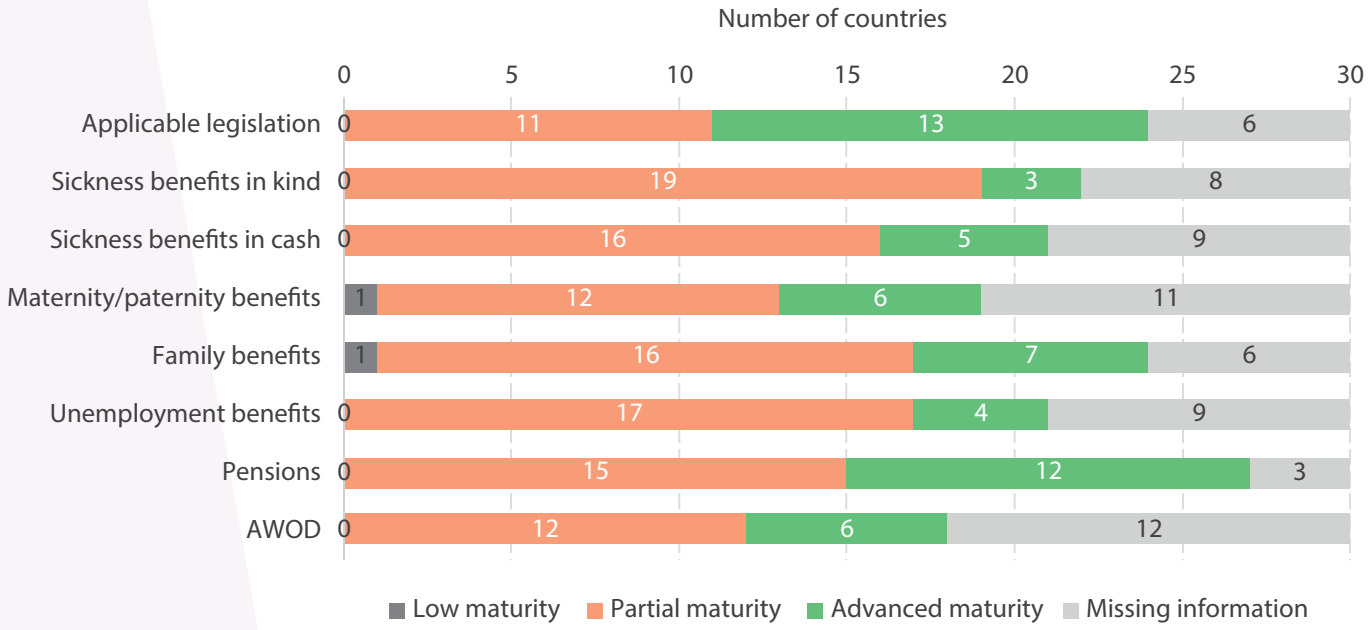
Partial digital maturity

Anvanced digital maturity

4.2. Trends in digital maturity of services across social security branches

Digitalisation initiatives of social security services beyond those required by EU legislation are typically driven at the institutional level, rather than dictated by the social security branch. This is because Member States are organised differently in terms of the specific needs and challenges of individual institutions, with the provision of social security benefits in some countries being centralised by one of the country's main authorities (e.g. in Spain, Italy and Latvia) and, in other countries, being split across several organisations (both public and private). Conversely, some Member States with higher numbers of cross-border workers have greater incentives to digitalise cross-border coordination and request procedures, aiming to reduce the burden of their workload and facilitate the process for local employers. It is important to note that this can lead to disparities in digital maturity across different branches and regions. Institutions often develop digitalisation strategies based on their unique requirements and resources, resulting in varying paces and extents of digitalisation, even within the same country. This institutional-level approach can pose challenges when it comes to cross-border integration and data sharing. Figure 2 shows the digital maturity of the different social security branches and the variance across Member States.

Figure 2. Digital maturity of cross-border services in Member States by social security branch



Source: Milieu Consulting, based on its own DMA.

Among the different social security branches included in the scope of this study, **pension services often demonstrate a high level of digital maturity** in many Member States, especially in the accessibility and interoperability dimensions. This advancement is driven by several factors. Pension services are among the most commonly used social security benefits, serving a large portion of the population. This high volume of users justifies significant investment in digital infrastructure. Furthermore, pensions are particularly relevant for cross-border users, such as individuals who have worked in multiple countries throughout their careers or who move abroad after retirement. In 2023, for instance, 6.3 million pensions were paid to beneficiaries residing in another Member State, amounting to a total of EUR 28.4 billion ([84]). Advancing digitalisation in this sector therefore makes sense, as it facilitates the often-complex process of aggregating and coordinating pension rights across borders, in compliance with Regulations (EC) No 883/2004 and No 987/2009. The long-term nature of pension management and distribution also benefits from digital systems that can efficiently handle complex calculations and long-term data storage.

The development of tools for determining **applicable legislation** and **issuing A1 PDs also shows advanced digital maturity**. This can be explained by the fact that determining applicable legislation is a necessary step before other forms of social benefits can be claimed. In 2023, a total of 5.5 million A1 PDs were issued in the EU, with 1.7 million of those being

([84]) European Commission: Directorate-General for Employment, Social Affairs and Inclusion, *Cross-border Old-age, Survivors' and Invalidity Pensions – Report on portable documents P1 – Reference year 2023*, Publications Office of the European Union, Luxembourg, 2025, https://employment-social-affairs.ec.europa.eu/policies-and-activities/moving-working-europe/facts-and-figures-intra-eu-labour-mobility-and-eu-social-security-coordination_en

issued to people active in two or more Member States and 3.6 million to posted workers ([85]). Moreover, determining the applicable legislation (and the related payment of social security contributions) has significant financial implications for Member States and is therefore regarded as a sensitive aspect of social security coordination. Finally, the digitalisation of requests for and decisions on A1 PDs is also provided for under the SDGR (in Annex II, which lists the procedures to be offered fully online, in accordance with Article 6(1)).

Online applications for an **EHIC** are also required under the SDGR, which explains their implementation across Member States. The relatively straightforward nature of EHIC requests makes them well suited for digitalisation, all creating a strong incentive for efficient digital request processes. In 2023, around 48 % of EU, European Free Trade Association and UK citizens were in possession of an EHIC, with a total of 253 million cards currently in circulation ([86]). Notably, as this report has shown, several Member States now also offer the provisional replacement certificates for lost or unavailable EHICs in a digital format.

In conclusion, although digital maturity is more significantly dictated by the resources and needs of national-level social security institutions, branch-specific advancements are often propelled by a combination of high utilisation, cross-border relevance, regulatory requirements and the potential for significant efficiency gains. As digitalisation efforts continue, it will be crucial to foster knowledge sharing and best practices across institutions to ensure a more uniform progression of digital maturity across all social security branches.

4.3. Main benefits and challenges in further advancing digital maturity of cross-border services

The European Commission's 2023 communication on digitalisation in social security coordination ([87]) advocates for the acceleration of efforts to implement a modern, integrated digital system of social security coordination in the EU. The primary objective of advancing digitalisation in this field is to facilitate a seamless and secure flow of information across borders for national authorities to coordinate citizens' social security rights and benefits. This aids the prevention of fraud and streamlines administrative procedures, alleviating the burden for national authorities and their businesses partners offering services abroad. Additionally, accurate and efficient processing of social security data simplifies the delivery of social security services for mobile workers, ensuring that they have access to the social protection they are entitled to when moving or working abroad. Ultimately, these measures facilitate free movement in the single market, thereby stimulating sustainable growth and enhancing competitiveness in the EU.

Digitalisation in cross-border operations was reported as being generally well received among social security institutions, with the benefits of advancing these initiatives being widely understood and appreciated across social security branches. This positive reception paves the way for further progress in modernising cross-border social security systems. As institutions increasingly recognise the potential for improved efficiency and service delivery, the momentum for digital transformation continues to grow.

The following are the main advantages of digitalisation that were identified by institutions, and these factors have the ability to transform the efficiency and effectiveness of these critical services:

- **Enhanced efficiency and resource optimisation.** Digitalisation streamlines operations, leading to faster processing times and a reduction in the internal resources required. By automating routine procedural aspects of benefit evaluation and granting, caseworkers can redirect their focus to more complex and delicate aspects of their roles. This shift not only improves overall productivity but also allows a more nuanced approach to be taken to challenging cases.
- **Improved accuracy through data matching.** Digital systems excel at data matching, significantly reducing errors in the application and assessment process. Advanced algorithms can cross-reference multiple data points instantly, ensuring a more comprehensive and accurate evaluation of each case. Moreover, digitalised platforms can be designed to require applicants to provide all of the necessary information upfront, reducing delays caused by incomplete applications and improving the overall quality of the data submitted.

([85]) European Commission: Directorate-General for Employment, Social Affairs and Inclusion, *Posting of Workers. Report on A1 portable documents issued in 2023*, Publications Office of the European Union, Luxembourg, 2025, https://employment-social-affairs.ec.europa.eu/policies-and-activities/moving-working-europe/facts-and-figures-intra-eu-labour-mobility-and-eu-social-security-coordination_en.

([86]) European Commission: Directorate-General for Employment, Social Affairs and Inclusion, *Cross-border healthcare in the EU under social security coordination – Reference year 2023*, Publications Office of the European Union, Luxembourg, 2025, https://employment-social-affairs.ec.europa.eu/policies-and-activities/moving-working-europe/facts-and-figures-intra-eu-labour-mobility-and-eu-social-security-coordination_en.

([87]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on digitalisation in social security coordination: Facilitating free movement in the single market, COM(2023) 501 final of 6 September 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A501%3AFIN.

- **Enhanced collaboration and data sharing.** One of the most compelling advantages of digitalisation in cross-border social security is the enhanced ability for institutions to collaborate and share data. This improvement occurs both at the national level and across borders. Seamless data exchange enables a more holistic view of an individual's circumstances, facilitating more informed decision-making and reducing the likelihood of fraudulent claims or unintentional oversights.

Nonetheless, there are several significant challenges involved in the digitalisation of cross-border social security systems. The following two points were raised across several Member States with regard to ongoing challenges in the digitalisation process:

- **Low strategic priority due to limited cross-border cases.** In many Member States, the relatively low number of cross-border cases compared with domestic cases often results in digitalisation initiatives being assigned a lower priority at the strategic level. When resources are limited, institutions may prioritise projects that have an impact on a larger portion of their user base, potentially delaying crucial advancements in cross-border digitalisation efforts.
- **Complexity of cross-border cases.** Certain aspects of cross-border social security remain highly technical and nuanced, necessitating human intervention. The intricacies of international agreements, varying national legislations and unique individual circumstances often require expert judgement that cannot be fully automated.

In conclusion, while the benefits of digitalisation in cross-border social security are substantial and far-reaching, the challenges posed by resource allocation and the inherent complexity of certain cases cannot be overlooked. Moving forwards, a strategic approach that addresses these challenges while maintaining a clear view of the benefits that digital tools and services can bring to cross-border social security coordination will be crucial for the successful advancement of digitalisation in this field. With this in mind, the next chapter of this report explores the issue of resource availability and shortages in further detail.

5. Assessment of resource availability/ shortages for implementing digital solutions

Key findings from this chapter: resource availability for implementing digital solutions

Many social security institutions face resource challenges in digitalising cross-border social security services. Among the primary shortages having an impact on digitalisation initiatives are a lack of IT skills and regulatory knowledge, particularly in cybersecurity and complex digital solutions, and a lack of funding, particularly when new technologies are perceived as having high implementation costs and the numbers of cross-border cases are low. However, there is variance across Member States, with each national context being limited by a different set of restraints.

The key priority areas for improvement, as identified by the social security authorities interviewed for this study, include:

- the improvement and interconnection of Member States' databases;
- enhancing user accessibility and efficiency through digital tools;
- fostering the automation of processes through, for instance, robotisation;
- strengthening data security by implementing modern cybersecurity solutions and training employees.

These priority areas are consistent with the dimensions of digital maturity contained in the DMA framework developed for this study. Furthermore, social security authorities have suggested that resource limitations be addressed and the digital maturity of their services be enhanced through several approaches. These include increasing outsourcing, staff training, fostering interinstitutional knowledge exchange and EU funding.

As the European Commission highlights in its 2023 communication on digitalisation in social security coordination ([88]), digitising public services is critical for building modern and efficient administrations. Indeed, various social security institutions across several Member states recognise that automation improves efficiency and frees up human resources by reducing processing times and boosting employee productivity, allowing staff to focus on more sophisticated tasks.

However, digitalising cross-border social security services also entails costs. First, adequate funding is needed to develop and sustain the necessary infrastructure. This includes not only the initial costs of implementing digital systems, but also the ongoing expenses for maintenance, updates and integration with other systems, ensuring they remain functional and secure in the long term. Second, institutions must ensure that they have sufficient staff with the appropriate skills to support these efforts. Digitalisation relies on advanced infrastructures, which demand the expertise of highly specialised professionals. Additionally, the complexity of the EU regulatory framework for social security coordination requires staff with in-depth legal and policy knowledge. Overall, these challenges can be particularly burdensome for institutions that are already struggling with limited resources and heavy workloads.

Meanwhile, the European Commission has worked to provide funding instruments to finance digitalisation of cross-border social security tools. For instance, in the 2023 communication on the digitalisation of cross-border social security, the importance of funding from the digital Europe programme, InvestEU, the European Regional Development Fund, the European Social Fund Plus and the Technical Support Instrument is underscored to support digital transition efforts in social security systems. Furthermore, as the Commission underlines, recovery and resilience plans need to allocate at least 20 % of their own resources to digitalising public administration services and processes. Finally, the DC4EU project, co-financed under the Digital Europe Programme, will allocate around EUR 19.2 million to support the application of the eIDAS trust framework in the education and social security field, engaging, for instance, in the execution of A1 and the EHIC documents ([89]). This project involves 43 public organisations in 22 Member States, Norway, Switzerland and Ukraine ([90]).

([88]) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on digitalisation in social security coordination: Facilitating free movement in the single market, COM(2023) 501 final of 6 September 2023, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A501%3AFIN.

([89]) For further information, see DC4EU (https://www.dc4eu.eu/) and European University Foundation, 'DC4EU', European University Foundation website, https://uni-foundation.eu/project/dc4eu/.

([90]) This figure also includes the institutions involved in the educational component of the project.

In the light of these difficulties and actions, this chapter addresses the issue of resource availability and shortages – in terms of both funding and human resources – and the investment priorities underscored by social security institutions in implementing cross-border digital solutions. It also explores the use of outsourcing, training and EU funding as potential avenues to tackle these challenges.

5.1. Availability of financial resources

As mentioned above, while digitalisation automates processes and frees up human resources, it requires a considerable amount of investment to be rolled out and sustained. This observation is equally relevant in relation to cross-border social security. The analysis shows that resource availability and needs vary across the Member States, with some institutions identifying the level of funding available to them as adequate, while other institutions reportedly face resource constraints to fully implement the necessary digitalisation efforts.

The **level of funding** allocated is deemed **adequate** by social security institutions in Ireland and Finland (institutions responsible for determining applicable legislation), Luxembourg, Malta and Norway (sickness and maternity/paternity benefits) and France (pensions). At the same time, while some institutions acknowledge an adequate level of resources, they also note that continued resources are always needed to further implement digitalisation efforts ([91]).

Other social security institutions across the various Member States report facing **resource constraints and challenges in securing funding** (e.g. CZ, EE, ES, HU, IS, LV and PT). For instance, the Spanish Social Security Institute reports that insufficient funding, particularly in international departments, creates challenges, adding to the complexity of the tasks involved. In the Hungarian institution delivering family benefits, financial difficulties, combined with a lack of specialists, pose obstacles to introducing digital procedures. The Latvian State Social Insurance Agency underlines that, despite the beneficial impact of digitalisation in reducing resource intensity and in optimising processes execution, initiatives are affected by the unavailability of funding.

The **high cost of implementing digital solutions and specific technological tools** further exacerbates the issue for many institutions, making it difficult to allocate sufficient resources for the development and maintenance of digital systems. For instance, the National Health Insurance Fund of Bulgaria considers the high cost of new technologies as the primary obstacle for enhanced digitalisation. Similarly, the Lithuanian institution delivering sickness benefits notes that that the implementation of the electronic EHIC – with the possibility of healthcare providers checking the validity of EHICs and using their data to claim reimbursement – could be remarkably costly.

5.2. Availability of human resources and skills

Digitalising cross-border social security requires not only considerable financial resources, but also highly specialised human resources with relevant technical and regulatory expertise to implement advanced and compliant digital solutions.

A few social security institutions across different Member States affirm that **human resources in their institutions are sufficient** for the work of their organisations, in terms of the **number of people** involved in the implementation of digital tools and services. This is the case of certain institutions in Iceland, Malta and Norway. In terms of the skills required, a few institutions report that they consider **the level of skills as adequate for their organisation**. This was, for instance, the case in Ireland (applicable legislation), Hungary (in the field of family benefits) and Slovenia (health insurance). The Norwegian institution delivering sickness and AWOD benefits highlights good complementarity between the skills of the different employees working in the organisation.

However, **a considerable number of institutions report human resources and skills shortages**. While a number of organisations report a **general problem with staff shortages** – with often small teams responsible for day-to-day responsibilities facing difficulties in balancing these responsibilities with the development of digitalisation projects (e.g. LV, PT, SI, SK and FI), there are also institutions that indicated that they are running into more **specific skills shortages**.

The following competency areas are those where institutions are facing the biggest challenges:

- **IT skills.** A significant number of institutions across the Member States are experiencing challenges in relation to IT skills (e.g. in EE, IE, FR, LT, LU and PT). In particular, the combination of technical development skills and an understanding of social security issues and their complexity was mentioned as an important gap. However, specific IT skills were also sometimes lacking. For example, the Slovak Social Insurance Agency highlights the need to increase the number of IT and cybersecurity experts able to deal with complex digital solutions as one of its main challenges.

([91]) Interviews with stakeholders from Luxembourg and Norway.

- **Business process and managerial skills.** A number of institutions also identify gaps in relation to the project management skills or business process skills needed to implement and run often lengthy and complex digital solutions and digitalisation processes. This was, for instance, the case in Estonia, France, Italy and Luxembourg.
- **Combination of IT and regulatory expertise.** A significant number of institutions highlight the importance of combining technical development skills with regulatory expertise in the area of social security, pointing to a need for **multidisciplinary teams** involved in the implementation of digitalisation efforts. This was, for instance, raised by respondents in Estonia (family benefits, pensions and applicable legislation), France (unemployment benefits) and Ireland, Norway and Slovakia.
- **Language.** Finally, the lack of language skills of some civil servants was identified as a factor discouraging employees from participating in European coordination initiatives and leading to limitations in collaborating or negotiating with other countries (in Spain).

A few institutions also suggest some potential factors that could explain and reinforce such skills shortages:

- **High labour costs and turnover.** Employing people with the right skills can be expensive. For example, the Irish institution in charge of sickness benefits notes that specialist roles cost more than administrative roles in terms of full-time equivalents. Furthermore, some institutions face challenges in retaining employees due to high turnover rates. This is the case of France (unemployment benefits) and Italy (pension benefits). This might have an impact on the development of on-the-job skills, as mastering certain tools and procedures takes time.
- **Low wages and rigid selection procedures.** In countries such as Poland and Slovakia, low wages in the public sector are mentioned as a major obstacle in hiring skilled personnel. Furthermore, some institutions note that their long and rigid recruitment processes complicate hiring procedures, such as in Ireland (sickness benefits) and Italy (pensions). The former claims that recruitment processes can take from three to six months.
- **Competition with the private sector.** This might represent another obstacle in attracting talented employees. The Dutch Employee Insurance Agency, while observing no major issues in attracting people with the right skills profiles, underlines that it is experiencing a challenge in terms of competition with salaries offered by the private sector for IT roles. In a similar vein, the Norwegian Labour and Welfare Directorate notes that competition for hiring skilled developers is becoming increasingly fierce.

5.3. Priority resources and investment needs identified

Priority resources and investment needs has been broadly identified on the basis of the interviews. The resulting list of priority areas intends to provide a first-hand overview of areas where additional resources may be needed as a priority in this context, based on the experience of the civil servants involved in the day-to-day coordination of social security coordination and/or the development of digital tools and solutions.

The resource and investment needs identified align to a large extent with the assessment of digital maturity performed in the report, identifying priority actions and areas relating to data integration, automation, user accessibility and error/fraud detection.

The following priority resource and investment needs were identified:

- **Database and infrastructure development.** Improving existing infrastructure and databases and ensuring their cross-border interoperability constitutes a key priority to improve cross-border social security services. Several institutions stress the need to improve and maintain databases while integrating them with other systems (AT, EE, IS and SK). For example, in Austria, ÖGK highlights the integration of regional insurers and IT systems as a major challenge. Estonia's Social Insurance Board calls for the modernisation of its health insurance fund database and its integration with EESSI, while in France only unemployment benefits and cost reimbursement processes have an integrated solution in EESSI. Luxembourg's institution dealing with family benefits has identified the determination of datasets for seamless reciprocal exchange with other Member States and the creation of a unique European identifier as challenging. This is because data exchange must be reciprocal, requiring all of the parties to agree on exchanging information. The Slovak Social Insurance Agency, meanwhile, emphasises the need to modernise IT infrastructure and ensure interoperability and support. Data quality is also a priority for institutions in Belgium and Slovakia, with the Belgian institution stressing the need to invest in preventing duplicate data entries. It is important to note, in this context, that the further integration of databases and infrastructure needs to take into careful consideration the challenges identified in this report regarding legacy infrastructure and the comparability of datasets (Section 4.3; for example, definitions). These challenges require the harmonisation of datasets' interoperability requirements, such as the adoption of common data formats and standards across Member States' institutions, and of security procedures.

- **Improved user accessibility.** Making the delivery of cross-border social security services accessible to users is a major priority for several institutions across different Member States (AT, CZ, LV, NO, PT and SK). For example, the Norwegian National Insurance Scheme argues that, for pension benefits, a priority should be the development self-service digital solutions allowing cross-border users to provide information directly without using paper forms.
- **Automation.** Automating processes is a priority for a number of social security institutions. This issue is explicitly mentioned as a priority issue in Belgium, Czechia, Iceland, Latvia, Norway and Slovakia. Belgium has undertaken pilot projects in recent years to deploy automation (robotic process automation) for administrative tasks, such as the uploading of documents in electronic document management systems or the selection and use of information across documents. The Norwegian National Insurance Scheme calls for the development of automated systems to exchange information regarding periods of work or insurance across different Member States, facilitating the aggregation of this information to calculate pension benefits.
- **Data security.** Ensuring that personal data are protected in the right way is a priority for social security institutions in Denmark, Norway and Slovakia. According to the Slovak Social Insurance Agency, this should entail investment in moder cybersecurity technologies, data encryption to protect data during transmission and storage, appropriate training for employees and compliance with relevant regulations, such as the GDPR.
- **Other investment priorities.** Among other priorities, the creation of a **specialised department for international issues** was highlighted by the Spanish Social Security Institute and more investment in **training** was highlighted by the French institution dealing with unemployment benefits. Training in cybersecurity is one of the key priority areas of the Slovak Social Insurance Agency. Finally, the CSSA in Czechia underlines the **implementation of more coordinated planning** as one of its priorities.

5.4. Strategies to address shortages

As this report has documented, financial and human resources shortages constitute a significant issue for several social security organisations. Organisations have developed different ways to overcome such challenges. The following are the four main solutions identified in the interviews with social security institutions:

- **Outsourcing.** Subcontracting external companies to handle certain tasks is one approach employed to address labour shortages, although it can be costly for organisations. Social security institutions in Czechia, Malta, the Netherlands, Portugal and Slovakia have reported using outsourcing. In Czechia and Slovakia, this specifically involves outsourcing employee training**.**
- **Training.** On-the-job training programmes represent a way to address skills shortages, allowing employees to update their knowledge of digital tools and of cross-border regulations. However, as in the case of outsourcing, it can be too expensive for organisations already struggling with funding. The use of training programmes was explicitly reported by social security institutions from Czechia, France, Luxembourg, Malta, Portugal, Slovenia and Slovakia. However, a challenge of training lies in the fact that employees have limited time to learn complex subjects. This is underlined, for instance, by the Luxembourgish institution delivering sickness, family and maternity and paternity benefits.
- **Knowledge exchange among institutions.** The cross-border exchange of best practices allows social institutions to create synergies, improve their knowledge and make efficient use of resources. However, participating in cross-border forums demands both financial and human resources. A number of institutions report some form of exchange with other Member States or participation in cross-border projects. The DC4EU initiative, in which Germany, Italy, Austria and Finland participate, is a good example. The Austrian Social Insurance System engages in international projects focusing on digital transformation processes within e-government.
- **EU funding.** The use of EU instruments to fund innovative digitalisation projects can be another route to overcome financial challenges. A number of organisations report the use of EU funding, coming mostly from the recovery and resilience plans (e.g. in Czechia and Italy). The CSSA in Czechia deems this line of funding to be critical for the continuation of services and expects challenges after 2025, when this particular form of funding will end. In Italy, funding from the national recovery and resilience plan has been used to implement an innovative digital tool, the IT Wallet of the IO app, that is, a digital wallet that will allow users to access all of the country's public administration services and to upload documents, including for the EHIC ([92]). However, Italy and Austria note that securing funding for EU initiatives may be challenging for social security organisations due to a lack of knowledge on EU funding procedures or a lack of resources available to prepare applications.

([92]) SkyTg24, 'IT Wallet: cos'è, quali documenti contiene, quando arriva il "portafoglio digitale"' ('IT wallet: What is it, what documents does it contain, when is the "digital wallet" arriving'), SkyTg24 website, 19 September 2024, https://tg24.sky.it/tecnologia/approfondimenti/it-wallet-app-io?card=1.

5.5. Concluding remarks: resources and digital maturity

A good number of social security institutions across Member States experience resource challenges in digitalising cross-border social security services. Having adequate financial resources and the right technological and regulatory expertise is critical for the development of digitally mature cross-border solutions in the field of social security. These solutions are characterised by accessible electronic services, efficient digital administration, highly interoperable systems, secure networks and data-protection tools, and effective error- and fraud-detection systems.

The key resource priorities identified are the improvement and interconnection of Member States' databases; enhancing user accessibility and efficiency through digital tools; fostering the automation of processes through, for instance, robotisation; and strengthening data security by implementing modern cybersecurity solutions and training employees. It is worth noting that these priorities align quite well with the key issues addressed throughout the report, which constitute the centrepieces of its implementation analysis and DMA. Such alignment provides potential avenues for action at both the EU and the national levels to promote seamless and digitally mature integration between cross-border social security services.

The social security organisations interviewed hint at ways to overcome resource shortages and make cross-border services more digitally mature. Some of the options suggested include outsourcing, training, interinstitutional knowledge exchange and EU funding. However, each comes with limitations. Indeed, outsourcing, training and cross-border exchanges, while potentially effective in addressing human resources shortages, might prove costly for already resource-strained and understaffed social security institutions. Instead, EU funding, although potentially useful in funding digitalisation projects, is difficult to secure and requires skilled people to fully leverage its potential.

Annex A – Inventory of digital cross-border services in Member States

The inventory of cross-border digital services in the field of social security coordination covers the electronic, digital and online tools (both in production and under development) that enable or facilitate interactions between the administrations of Member States or between the social institutions and their clients (including claimants of benefits, recipients of benefits, employers and self-employed workers).

The inventory is presented in Excel format, consisting of one sheet per country. The information for each country is organised by the social security branches covered in the study:

- sickness benefits in kind,
- sickness benefits in cash,
- maternity/paternity benefits,
- family benefits,
- unemployment benefits,
- pensions,
- AWOD.

Moreover, a specific line was added on 'applicable social security coordination' to allow national experts to indicate when a tool or a service is put in place for determining the applicable social security legislation. The objective of this tool, then, could also be to detect fraud and to verify the validity of A1 PDs.

Table 7 sets out how the inventory is structured ([93]).

Table 7. Information gathered as part of the inventory

A. Cross-border digital services in the area of	The applicable social security branch: sickness benefits in cash, sickness benefits in kind, maternity benefits, paternity benefits, maternity and paternity benefits, family benefits, unemployment benefits, pension benefits, accidents at work benefits, occupational diseases
B. Name and hyperlink (if any)	
C. Main objective	Obtain a benefit, provide a benefit, obtain a PD, deliver a PD, verify a PD, detect relevant changes in personal circumstances, exchange information, assess risk, match data, withdraw PD
D. Type	
Electronic	It is a tool that works through a chip (e.g. a card allowing you to pay in a contactless manner)
Online	It is a platform/database/portal/etc., available online (e.g. a portal where you can calculate the amount of your pension in 10 years)
Digital	It is an app / a station that uses technology to provide a service, not necessarily online (e.g. an app on your phone or a self-service ordering kiosk where you can order and pay for food without interacting with a person)
E. Status	Used, under development
F. Facilitates interaction between	Administrations of Member State institutions and users
G. Description of the tool	
H. This service uses automated processes	Meaning that, for instance, the service you are describing is using physical machines, computer software and other technologies to perform tasks that are usually done by humans (e.g. a fraud-detection algorithm or chatbot)
I. Comments	

([93]) The inventory primarily concentrates on specific services relevant to each branch of social security. Therefore, overarching digital tools that may be used across multiple branches are not included as stand-alone elements to avoid repetition. This focus might result in a fragmented view that overlooks integrated or multifunctional digital solutions.

Annex B – Interviews conducted and social security branch coverage

Member State	Participating institutions	Applicable legislation	Sickness benefits in kind	Sickness benefits in cash	Accidents at work and occupational diseases	Maternity/ paternity benefits	Family benefits	Unemployment benefits	Pensions
AT	ÖGK Dachverband der österreichischen Sozialversicherung (Umbrella Organisation for Austrian Social Security Authorities)		x	x	x	x	x		x
BE	National Social Security Office Federal Agency for Occupational Risks (Fedris) Agentschap Uitbetaling Groeipakket (VUTG) Service fédéral des pensions (SFPD)	x	x		x		x	x	x
BG	National Health Insurance Fund		x		x				
CY	Ministry of Health Ministry of Labour and Social Insurance Deputy Ministry of Social Welfare	x	x	x	x	x	x	x	x
CZ	CSSA Ministry of Labour and Social Affairs Labour Office of the Czech Republic	x		x		x	x	x	x
DE	Deutsche Rentenversicherung Bund (German Pension Insurance Institute) Bundesagentur für Arbeit (BA)							x	x
DK	Udbetaling Danmark	x							x
EE	Estonian Social Insurance Board Estonian Health Insurance Fund	x	x	x		x	x		x

Member State	Participating institutions	Applicable legislation	Sickness benefits in kind	Sickness benefits in cash	Accidents at work and occupational diseases	Maternity/ paternity benefits	Family benefits	Unemployment benefits	Pensions
EL	Ministry of Labour and Social Security e-EFKA (Electronic National Social Security Entity)	x	x	x	x	x	x	x	x
ES	National Social Security Institute	x	x	x	x	x	x	x	x
FI	Tapaturmavakuutuskeskus (TVK, Finnish Workers' Compensation Center) Finnish Centre for Pensions (ETK) Kela	x	x	x	x	x	x	x	x
FR	CNAF Caisse Nationale d'Assurance Maladie - CNAM Caisse Nationale d'Assurance Vieillesse - CNAV France Travail						x	x	x
HR	Croatian Pension Insurance Institute (HZMO)	x							x
HU	Ministry of Interior, Department of Social Affairs Ministry of National Economy, Department of Employment Services Hungarian State Treasury, Pension Insurance Administrative Department						x	x	x
IE	Department of Social Protection Health Service Executive	x	x	x					
IS	Vinnumálastofnun (VMST, Icelandic Health Insurance) Directorate of Labour Social Insurance Administration	x	x					x	x
IT	National Social Security Institute (INPS)			x		x	x	x	x
LI	Office of Public Health		x	x	x				

Member State	Participating institutions	Applicable legislation	Sickness benefits in kind	Sickness benefits in cash	Accidents at work and occupational diseases	Maternity/ paternity benefits	Family benefits	Unemployment benefits	Pensions
LT	State Social Insurance Fund Board National Health Insurance Fund under the Ministry of Health (NHIF) Sodra	x	x		x	x		x	x
LU	Caisse pour l'Avenir des Enfants Agence pour le Développement de l'Emploi (ADEM) Association d'assurance accident National Health Fund (CNS) Caisse nationale d'assurance pension (CNAP)		x	x	x	x	x	x	
LV	National Health Service State Social Insurance Agency		x	x	x	x	x	x	x
MT	International Relations Unit Department of Social Security (DSS)		x	x	x	x	x	x	x
NL	CAK Social Verzekeringsbank (SVB) Het Uitvoeringsinstituut Werknemersverzekeringen (UWV)		x		x		x		x
NO	Directorate of Health National Insurance Scheme of Norway Directorate of Labour and Welfare	x	x	x	x	x	x	x	x
PL	Social Insurance Institution National Health Fund Ministry of Family, Labour and Social Policy	x	x	x			x	x	
PT	Social Security Institute	x	x	x	x	x	x	x	x

Member State	Participating institutions	Applicable legislation	Sickness benefits in kind	Sickness benefits in cash	Accidents at work and occupational diseases	Maternity/ paternity benefits	Family benefits	Unemployment benefits	Pensions
RO	National Agency for Payments and Social Inspection						x		
SE	Swedish Social Security Agency (Försäkringskassan) Swedish Pensions Agency (Pensionsmyndigheten)		x	x	x	x	x	x	
SI	Employment Service of Slovenia Health Insurance Institute of Slovenia Pension and Disability Insurance Institute of Slovenia		x			x	x	x	x
SK	Social Insurance Agency			x	x	x	x	x	x

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

On the phone or in writing

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- at the following standard number: +32 22999696,
- via the following form: european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU publications

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

EU open data

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

European Labour Authority
Landererova 12, 811 09
Bratislava - Slovakia

www.ela.europa.eu
https://www.facebook.com/europeanlabourauthority
@EU_ELA
https://www.linkedin.com/company/european-labour-authority
instagram.com/eulabourauthority

Publications Office of the European Union

Printed by [Xxx] in [Country]
Luxembourg: Publications Office of the European Union, 2023

PDF: ISBN 978-92-9401-865-6 | doi:10.2883/8947256 | HP-01-24-004-EN-C