

E-SOCIAL SECURITY: ANTICIPATING THE FUTURE ESIP Conference 2018

Scoping paper

Workshop 1: Digital tools for information exchange between social security systems

Moderator: Elise Debiès, Director of International Relations at French Old-Age Statutory Institution (CNAV)

In May 2015, the European Commission launched its Digital Single Market Strategy, as part of its ten main political priorities and this has led to the publication of a vast range of initiatives. Amongst them, of major interest for social security institutions is the new e-Government Action Plan, to accelerate the digital transformation of governments and public administrations (underlying principles of initiatives to be launched as part of this e-gov Action Plan in the background information (1) to this scoping paper).

Information exchange between social security systems are a significant part of a better service delivery to citizens. The best social security service is probably when systems do exchange information, after informing or getting express consent of citizens, so that citizens do not need to provide the same information twice (once only principle), or even do not need to provide any information at all (the information is produced or collected by a public institution).

The latter is being achieved for example in the field of life status information data exchange: the production of life certificates by citizens is progressively replaced by data exchange between institutions, achieving more security reliable and trustworthy information institutions, without unnecessarily bothering citizens. Another example are social insurance statements, such as amounts of contribution, which can be exchanged or accessed in adequate security conditions.

Sharing common systems for citizens' identification is key to allow the exchange of data between social security institutions. This requires at least table of correspondence between the different national identification systems or could be further tackled through the use of a European Social Security Number, as was discussed by the European Commission.

However, most of the time, before such automatic data exchange is put in place between institutions, an active involvement of citizens is still needed to enforce their rights, by asking them to justify their identity and situation. In this case, social security institutions should be able to cooperate further so that, in case another European institution is

ESIP aisbl

Maison Européenne de la Protection Sociale

Rue d'Arlon 50 • 1000 Bruxelles • ☎ +32 2 282 05 60 • 📠 +32 2 282 05 98

✉ esip@esip.eu • 🌐 www.esip.eu • 🐦 @ESIP_EU • VAT: BE 0808.072.950

involved, the technical and legal interoperability of our systems do guarantee the once only principle.

In order to tackle these issues, we propose to divide the workshop in 3 groups dealing with the following topics:

1- Conditions to meet for coming into force of the principle “once-only” between European social security systems.

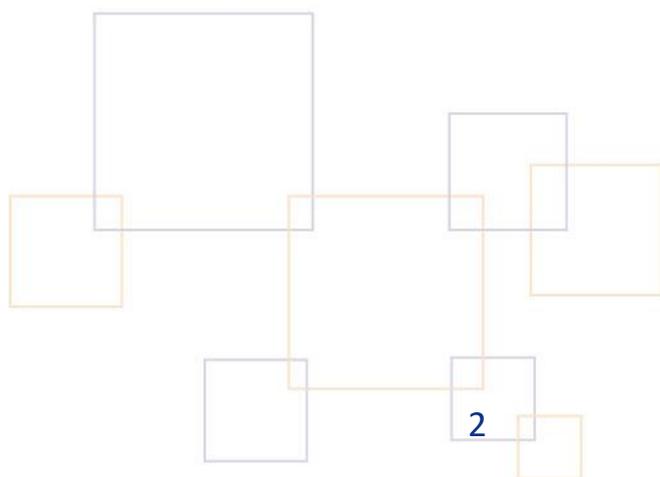
The new gateway will help to reduce administrative burdens. As a general rule, the single digital gateway will apply the "once-only" principle, which means that individuals and businesses will only have to supply the same information once to public administrations. The functioning of the gateway will be supported by technical tools developed by the Commission in cooperation with national administrations.

2- EU-level interoperability solutions: what could be an optimal combination of EU level information exchange systems (like EESSI) and progressive extension of bilateral data exchange through common standards (like death data exchange)?

Additional question on optimizing data exchange: to which extent can social security institutions make the most of the data already available for exchange (including before the official EESSI implementation),

3- Information and consent of citizen to data exchange between social security institutions: what level of transparency of information is desirable (see end of background information, 2)?

Additional question on data protection: What could be the right balance between fulfilling missions of social security institutions and complying with data protection requirements at EU and national level?



Background Information: European Commission E-Government Action Plan

1-Initiatives to be launched as part of the e-Gov Action Plan should observe the following underlying principles:

- **Digital by Default:** public administrations should deliver services digitally (including machine readable information) as the preferred option (while still keeping other channels open for those who are disconnected by choice or necessity). In addition, public services should be delivered through a single contact point or a one-stop-shop and via different channels.
- **Once only principle:** public administrations should ensure that citizens and businesses supply the same information only once to a public administration. Public administration offices take action if permitted to internally re-use this data, in due respect of data protection rules, so that no additional burden falls on citizens and businesses.
- **Inclusiveness and accessibility:** public administrations should design digital public services that are inclusive by default and cater for different needs such as those of the elderly and people with disabilities.
- **Openness & transparency:** public administrations should share information and data between themselves and enable citizens and businesses to access control and correct their own data; enable users to monitor administrative processes that involve them; engage with and open up to stakeholders (such as businesses, researchers and non-profit organisations) in the design and delivery of services.
- **Cross-border by default:** public administrations should make relevant digital public services available across borders and prevent further fragmentation to arise, thereby facilitating mobility within the Single Market.
- **Interoperability by default:** public services should be designed to work seamlessly across the Single Market and across organisational silos, relying on the free movement of data and digital services in the European Union.
- **Trustworthiness & Security:** All initiatives should go beyond the mere compliance with the legal framework on personal data protection and privacy, and IT security, by integrating those elements in the design phase. These are important pre-conditions for increasing trust in and take-up of digital services.

2-Opening the data and services between public administrations within and across borders will increase their efficiency and facilitate the free movement of businesses and citizens.

Citizens' lives have become increasingly digital, leading to higher expectations of public administration performance. Users wish to understand how the service works and they expect greater transparency. Furthermore, by opening up to and engaging with



stakeholders in decision-making, public administrations will become more trustworthy and more accountable. In addition, opening public sector data and services to third parties, in full compliance with the legal framework for the protection of personal data and for privacy, can contribute to growth and competitiveness.

