European Platform
tackling undeclared work

Seventh plenary meeting of the European Platform tackling undeclared work

Report on data protection and data exchange

October 2019

LEGAL NOTICE

Neither the Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the following information.

The information contained does not necessarily reflect the official position of the European Commission.

This document is part of the work programme 2019-2020 of the European Platform tackling undeclared work established through Decision (EU) 2016/344.

For any use of material which is not under the European Union copyright, permission must be sought directly from the copyright-holder(s) indicated.

This publication has received financial support from the European Union Programme for Employment and Social Innovation "EaSI" (2014-2020). For further information please consult: http://ec.europa.eu/social/easi

Table of contents

1 INTRODUCTION 1
2 ENHANCING DATA PROTECTION AND DATA EXCHANGE IN A CHANGING CONTEXT .. 1
2.1 State of play 3
2.2 The GDPR imperative 4
2.3 Pioneering experience of data exchange for tackling undeclared work 5
3 DATA EXCHANGE AND DATA PROTECTION IN TACKLING UNDECLARED WORK: TOOLS, CHALLENGES AND CORRECTIVE MEASURES 8
3.1 Tools for cross-border data exchange 9
3.2 Data protection challenges for cross-border data exchange 11
3.3 Measures to address data protection and data exchange challenges 11
4 ADDRESSING DATA PROTECTION MYTHS: EVOLUTION OF NATIONAL INSTITUTIONAL RESPONSES 12
5 CONCLUSIONS AND THE WAY FORWARD 14

1 INTRODUCTION

The seventh plenary meeting of the European Platform tackling undeclared work (the Platform) was held in Brussels on 24-25 October 2019. The first day of the plenary was dedicated to a thematic discussion on data protection and data exchange for tackling undeclared work. This report summarises the presentations and discussions at the thematic day. It draws upon the input paper prepared for the meeting [1], a more detailed analytical paper for internal use in the Platform, as well as findings from the Annual Platform Survey and the Platform Working group 'Developing an IMI module for UDW/data sources and tools for inspectors'[2].

The thematic day consisted of an introductory panel discussion, followed by two parallel workshops respectively focusing on the following key questions:

- Plenary: How has data exchange for the purpose of tackling undeclared work evolved, in a context marked by increasing concerns for data protection and new technological opportunities?
- First workshop: What successful practices and tools for data exchange for tackling undeclared work have been implemented in your country that might be transferable to other Member States or the EU?
- Second workshop: What are the key data protection challenges that your enforcement body faces and what national and EU level measures could help alleviate them?

The thematic day aimed to explore the main challenges, tools, practices and the way forward on data protection and data exchange in tackling cross-border undeclared work. It sought to deepen the Platform members' common understanding of how to protect and use data, showcase examples of promising tools and practices, and define measures, which can help address the key existing challenges.

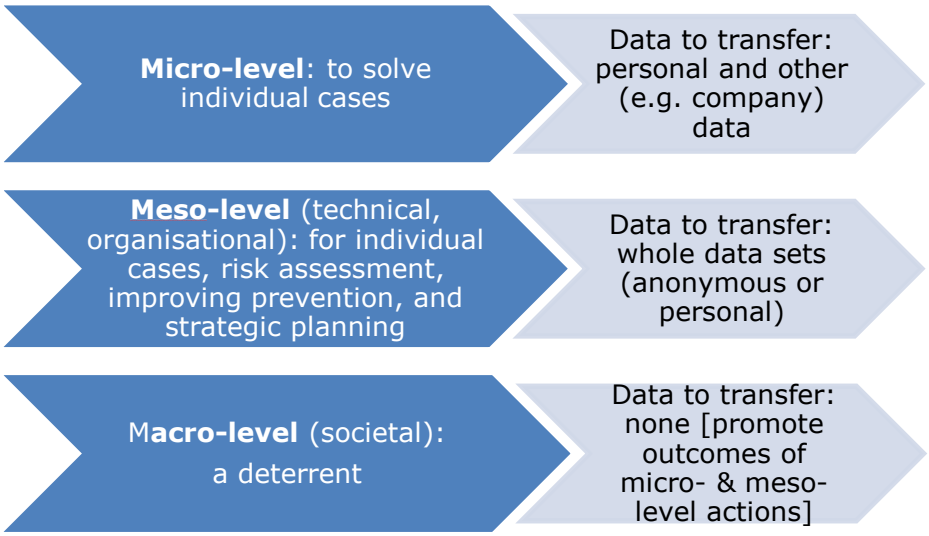
2 ENHANCING DATA PROTECTION AND DATA EXCHANGE IN A CHANGING CONTEXT

Data exchange on national and cross-border level is essential for tackling undeclared work on three different levels:

- Micro-level (case-related): for carrying out inspections or investigations to solve individual cases. It typically involves limited data transfer of single files on persons or companies. It could also involve though direct access to other countries' databases or cross-border data matching for risk profiling in specific cases.
- Meso-level (technical, organisational): for risk assessment, increasing efficiency of inspections, improving prevention, and strategic planning; it thus enhances the capabilities for solving of individual cases. It requires data transfer of whole data sets or the integration of different data-sets.
- Macro-level (societal): for advertising the outcomes of micro- and meso-level actions. It typically does not involve actual transfer of data but a promotion and visibility of the impact of the first two levels.

[1] Stefanov R., el. Al. (2019). Enhancing data protection and data exchange in a changing context. Input paper to the thematic discussion. European Platform tackling undeclared work Plenary meeting 24-25 October 2019. (Not published).
[2] Discussion at the Working group on Developing an IMI module for UDW/data sources and tools for inspectors (23 May 2019, Brussels).

Figure 1. Hierarchy of reasons for data exchange



Source: Based on presentation from Professor Colin Williams, University of Sheffield, Seventh Plenary of the European Platform tackling undeclared work, 24-25 October 2019, Brussels.

Such data exchange invariably includes "personal data", which is subject to special data protection rules. Hence, for data exchange to be effective for tackling undeclared work enforcement bodies need to ensure adequate data protection on every step of the process of collecting, storing, processing and/or transferring of such "personal data". Each of the levels outlined above requires different capacities, tools and practices, and presents a different set of challenges to enforcement authorities. The rapid penetration of digital technologies in all spheres of life have created new opportunities for collecting, storing and transferring data for tackling undeclared work. But they have also added considerable concerns among enforcement bodies regarding data protection as technological complexity has increased the risk of unauthorised breaches and access to collected personal data.

Box 1. Definition of "personal data"

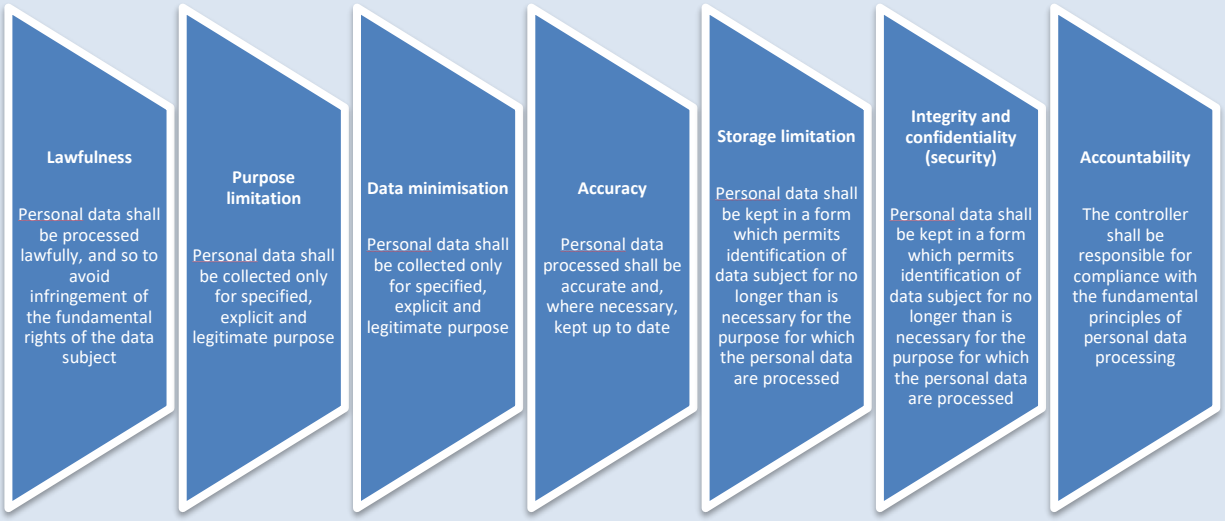
"Personal data" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Source: Article 4 (1) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR).

The EU has put together a comprehensive framework for data protection, which Member States need to heed and can rely upon in data exchange for tackling undeclared work. The key instrument Member States and enforcement bodies need to implement for guiding data protection and data exchange is the **General Data Protection Regulation (GDPR)**[3]. The GDPR updates and harmonises the EU approach to data protection and data exchange, responding to the promise and concern of new digitisation trends. It has, however, invariably put new requirements to Member States and enforcement authorities to update their data protection and data transfer rules.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

Box 2. GDPR Principles



Source: Based on Article 5 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR). Presentation of Kamil Košík, National Labour Inspectorate, Slovakia, Seventh Plenary of the European Platform tackling undeclared work, 24-25 October 2019, Brussels.

2.1 State of play

Data exchange for tackling cross-border undeclared work is currently mostly focused on ad hoc cooperation at **micro-level**. The tool most often used currently by enforcement bodies is the transfer of individual files, and it is typically done through the Internal Market Information (IMI) system.

Meso-level data exchange (whole datasets) is limited to national level, if at all, and is only rudimentary or at the pilot phase at cross-border level (e.g. between Belgium and the Netherlands). The exchange of or access to larger data sets across borders could be an important contribution to enhancing the tackling of undeclared work in the EU. Hence, discussions at the thematic day were particularly focused on how to ensure the wider and more effective use of big data for tackling cross-border undeclared work.

Consequently, the **macro-level** promoting of micro- and meso-level actions remain less well developed and focused on individual projects and their outcomes.

The results from the **2019 Platform survey**[4] confirm that there are **two main areas of general concern** expressed by enforcement authorities regarding data exchange, data protection and GDPR in tackling undeclared work[5]. The first relates to insufficient **knowledge** about the proper implementation of data protection rules (in their own country and in other Member States), resulting in a lack of understanding about what can or cannot be exchanged. The second concerns the lack of human (e.g., data protection officers) and technical (secure devices, encryption systems) **capacity**. The panel and the workshops of the thematic day of the Platform plenary provided examples and ideas of how these concerns and related challenges can be tackled more effectively by the Member States and the EU.

[4] European Platform tackling undeclared work. (2019). Annual Platform Survey. Tackling undeclared work in the collaborative economy and bogus self-employment, data exchange and data protection, and cross-border sanctions.
[5] Key conclusions from the Working group on 'Developing an IMI module for undeclared work, data sources and tools for inspectors' (23 May 2019, Brussels). Unpublished.

The panel discussions, as well as question and answer sessions have confirmed these general concerns and provided further glimpses into specific challenges concerning data protection and data exchange for tackling undeclared work:

- The effectiveness of GDPR in enabling data exchange depends on **the national legal database**. GDPR itself is not sector or technology specific and for enforcement bodies to be able to store and exchange information effectively, their public interest and official authority need to be well spelled-out in national legislation. Similarly, social partners have noted that for them to be able to play a bigger and more constructive role in data exchange it needs to be elaborated in national legislation.
- Both enforcement authorities and social partners have noted that there is an inherent trade-off between using anonymised and pseudonymised personal data for big data exchange and its usefulness for **risk profiling undeclared work**. Anonymised data are where a person cannot be identified from the data; pseudonymised data is where personal identifiers have been replaced by alternatives (e.g. names replaced with numbers) but contains personal data which could be used to identify a natural person, in which case, GDPR applies to them in full. For big data to be used for risk profiling and for building up cases for tackling undeclared work, this needs to be specifically foreseen in the law. It has been noted that the Platform has developed a body of knowledge on risk assessment (including a toolkit), and that risk assessment (on issues of cross-border labour mobility) falls within the tasks of the European Labour Authority.

2.2 The GDPR imperative

The thematic day included a general introduction from DG Justice and Consumers on the GDPR. **GDPR is a binding law**. Its effectiveness in general, and in particular for tackling undeclared work, depends to a large extent on the level of integration of GDPR rules in national legislation. For example, national legislation has to make sure **the public interest in tackling undeclared work and the specific authorities vested in enforcement bodies are clearly defined** and allow for the collection and exchange of needed data, including across borders. The GDPR has a two-year adaptation timeframe, which allows enough time for national legislators and enforcement bodies to take full advantage of its provisions. In addition, it is not a new starting point. It is an evolution of previous law of existing Directives. For GDPR to function effectively, there is a need to build on the national legal and institutional base appropriately.

In addition to the binding rules of GDPR, the European Commission and the **European Data Protection Board** have designed and provided **guidelines for proper implementation of the GDPR**. Member States, enforcement authorities and social partners can use these guidelines to build and develop their data protection and data exchange tools and practices.

The GDPR sets some important **data protection principles** such as fairness, transparency, purpose limitation, data minimisation, actuality of data (need to have updated data), storage only as long as necessary, data security and prevention of leakages. The key to effective data protection and data exchange for tackling undeclared work is that the legal base (EU or Member State) sets legal obligation or clearly defines the interests of the public for collecting and processing data in the performance of the tasks of the enforcement body. The enforcement body (the data controller) must have **a mandate to perform this public task**, not just a definition of the public interest. Within the mandate it must be necessary to process data. Consent must be freely given and individuals can withdraw it at any time.

Member States and enforcement bodies, are advised to focus on some **recommended core elements** for developing an effective data protection and data exchange practice based on the GDPR:

- Ensure awareness that they are legally bound by GDPR obligations.

- Focus on building the capacity of Data Protection Officers.
- Use the available external assistance. In particular, the European and national data protection authorities can be consulted for developing Data Protection Impact Assessment procedures and in specific cases.
- Notify data protection breaches to the Data Protection Authority.
- Ensure the enforcement body has the capacity and is able to conduct a Data Protection Impact Assessment. Then use its findings to perform data gathering and data sharing in compliance with the GDPR.

2.3 Pioneering experience of data exchange for tackling undeclared work

The existence of a harmonised EU/EEA-wide legal base (GDPR) **offers opportunities** for Member State enforcement bodies tackling undeclared work to develop and enhance their data sharing legal base and practices and to create common procedures for data exchange and risk assessment. These opportunities can be further enhanced by the advent of big data and computing modelling capabilities, which can improve risk management and infringement detection of undeclared work, provided that adequate data protection is ensured. As a result, new models of data exchange have already emerged both **on a case-by-case basis** and **on a more systemic level** (shared access to databases, exchange of larger sets of data for data mining and risk analysis, etc.). Some of these have been presented in the panel and the workshops of the thematic day of the Plenary.

Belgium has been at the forefront of developing data exchange tools for tackling undeclared work on national level and piloting them across borders. The Social Intelligence and Investigation Service presented an overview of the Belgian social inspection landscape, its data protection standards, the data sources and tools used and the evolution of data exchange in tackling undeclared work, as well as the challenges related to cross-border data exchange.

Belgium has many different labour and social inspection services, which has called for the creation of the **Social Intelligence and Investigation Service**. Among other tasks, the service has more recently been mandated with **datamining and matching** as key element in combatting (cross border) fraud in implementation of specific action plans. Carrying out this task has required the adoption and implementation of strict data protection standards and has made the service consider different possible ways to carry out its mandate.

Following the introduction of GDPR, Belgium has adapted its national legislation. This adaptation has been seen as **an evolution not a revolution**. Belgium adopted a new framework law that had a broad general scope on data protection and adapted sectoral legislation (tax, security forces, police, social inspection, etc.). The social security legislation has been revised to allow the upgrading of the 1990 Crossroads Bank Law, which regulates the handling of traffic management between different databases. The new framework provision has allowed for data warehouse using datamining and data matching techniques. In addition, the Belgian Social Criminal Code has been refined to include GDPR-conforming exceptions on the data protection rights of persons when social fraud, including such related to undeclared work, has been detected. The code also regulates data exchange between different inspectorates. At cross border level, the data exchange is shaped by EU regulation of social security systems coordination[6] and by bilateral agreements.

Belgium's legal base, on data exchange, has been complemented by the development of **strong institutions for data sharing** at national level. The federal minister in charge of social fraud is also in charge of the digital agenda, administrative simplification and privacy. Belgium has developed one federal Data Protection Authority (DPA) and four sectoral or

[6] Regulation (EC) No 883/2004 of the European Parliament and of the Council of 29 April 2004 on the coordination of social security systems

regional DPAs. In addition, in 2018 an Information Security Committee has been conceived for data exchange deliberations.

Belgium has thus been able to **integrate many different data sources and tools** to tackle undeclared work, such as the national register, employer directory, different types of employment and social security-related declaration registers, etc. Each of these sources provides access to specific online register. The access to the information of all these is incorporated through the DOLSIS platform. It is **an internal IT platform** for all social inspection services introduced in 2005. It allows inquiries and integrated access to all the different databases, thus allowing the profiling of high-risk companies and development of risk assessments through cross checking of data.

Figure 2. Belgian UDW data sources and tools: overview

Source: Presentation from Bart STALPAERT and Leen VAN ASSCHE, Belgium, Seventh Plenary of the European Platform tackling undeclared work, 24-25 October 2019, Brussels.

While the DOLSIS platform experience puts Belgium among the pioneers of using larger scale data sharing among labour and social security authorities to tackle undeclared work, the country still faces a lot of **data exchange challenges**. For example, it has yet to develop the exchange of data between different 'branches' of the administration: labour law and social security, tax authorities, police and the judiciary. On cross-border lever Belgium is still predominantly relying on (indirect) exchange of files in tackling undeclared work cases. But there is an ongoing debate of experimenting and piloting (direct) cross-border access to Belgian data sources from other Member States (in particular from the Benelux countries). There are some important pre-requisites for such data exchange to become reality, including among others: obtaining data exchange permission from the Information Security Committee, obtaining approval for use of the Belgian national number (challenges include legal vacuum for foreign entities), and ensuring very high level of data protection meeting Belgian standards (including secured access management).

Spain presented its experience of **developing data sharing** for tackling undeclared work **based on the strategic document** National Plan on Decent Work 2018 – 2020. The

Spanish Labour and Social Security Inspectorate ITSS[7] has powers for data collection when investigating individual cases. The law authorises ITSS to carry out any investigation, examination, reconstruction or evidence. In particular it can request information; demand the identification of persons at their workplace; examine all types of relevant documentation at the ITSS public offices; and take samples of substances and materials; photographs, videos, recording images, drawing up plans.

Through the National Plan on Decent Work Spain established the **Anti-Fraud Tool Unit**, which aimed to strengthen cooperation in tackling fraud, nationally and across borders, including in relation to undeclared work. Achieving this goal also meant **introducing new and more sophisticated data exchange tools and practices**, including:

- Information exchange & joint analysis of data;
- Fraud profiles and data mining;
- Compliance with national and EU regulations on data protection;
- Maintain, improve and establish new institutional relationships, through collaborative agreements with other public national public administrations and stakeholders and with neighbouring countries
- Focus on posting and letterbox companies through joint inspections and exchange of information (data).

State, regional and local administrations and other public entities are obliged to supply the inspectorate with any data, reports and background information of significance within the scope of their powers, as well as to provide cooperation. In order to **respond to the requirements of the GDPR** the ITSS has convened a special working group, which aimed to:

- Adapt the models of documents and information to the GDPR.
- Develop data protection requirements, criteria and instructions for inspectors, sub-inspectors and administrative staff.
- Modify several forms to allow personal data processing.
- Register the inspectorate with the Government Transparency website.
- Introduce new specifications on the content of the reports, infringement records, etc. of the ITSS.

A critical though less well studied aspect of tackling cross-border undeclared work is the **use of evidence** gathered in one Member State by one enforcement body in another Member state by another enforcement body. The **ELA** regulation foresees that some of its core tasks will be the **timely exchange of information** between Member States and the of support the national authorities in carrying out concerted and joint inspections. In this context, Eurofound has carried out a study[8]:

- **Mapping the practice**, if existent, of joint cross-border labour inspections at EU Member State level by labour inspectorates of other competent authorities; and
- Analysing the question if evidence gathered during these inspections in one Member State may be used in national court, administrative or other proceedings in another Member State.

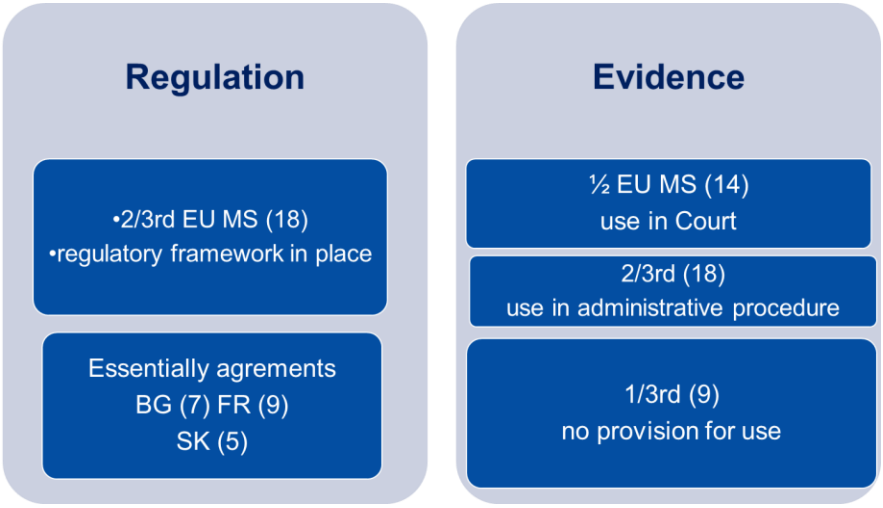
[7] Inspección de Trabajo y Seguridad Social.

[8] Through a survey of EURWORK correspondents who answered the key questions of (i) what regulations existed or practices on joint cross border inspections and (ii) what is known about how the evidence gathered can be used.

The study has revealed that the **use of evidence is not well established in national legislations** about exchange of information at cross border level. In some agreements, between enforcement bodies there is more information on what and how data can be gathered so that it can be used for evidence. in particular, this is true for the Benelux and Nordic countries. The IMI remains the tool of choice used for exchanging information. Some countries have underlined the difficulty to have the right format of the information to be presented in administrative or criminal court procedures in their country.

The Eurofound mapping found out that in relation to joint cross-border inspections around two-thirds of Member States (18) have a regulatory framework in place, while the rest rely on agreements only. Half of Member States (14) use **evidence in criminal procedures**, 18 use **administrative procedures**. Some one-third (9) of the Member States do not have legal provisions for using evidence on undeclared work. The differences in the legal regimes of treatment of undeclared work in the different countries results in a difference in the possible options of data exchange. This is further complicated by the possibility of an undeclared work case to start as an administrative investigation, which moves into the criminal domain and then is re-classified as administrative. In Germany, for example, in each of the phases, different legal possibilities for the exchange of data exist. There are many more possibilities for data exchange available in a case that is in administrative procedure than if the same case had entered criminal procedure. In the discussion following the Eurofound presentation Platform members and observers have noted that ELA can support the process of the use of evidence. This could happen by preparing model multilateral agreements, which would not require development of numerous bilateral agreements. An alternative and possibly less costly solution would be for Member States to align their national legislation to allow the use of evidence gathered in a cross-border context.

Figure 3. The use of evidence from joint cross-border inspections: legal base, administrative and criminal procedures



Source: Presentation from Isabella Biletta, Eurofound, Seventh Plenary of the European Platform tackling undeclared work, 24-25 October 2019, Brussels

3 DATA EXCHANGE AND DATA PROTECTION IN TACKLING UNDECLARED WORK: TOOLS, CHALLENGES AND CORRECTIVE MEASURES

The first workshop of the Plenary thematic day focused on identifying the key challenges and possible corrective measures to address them at national and EU level in relation to the tools for cross-border data exchange. Discussions were based on presentations of the experience and prospects of data exchange for tackling undeclared work in the

Netherlands, France and Portugal. They sought to identify successful practices and tools for data exchange for tackling undeclared work implemented in these countries that might be transferable to other Member States or the EU. The presentations focused in particular on:

- Data protection aspects in cooperation with Benelux countries, Netherlands.
- Transnational data exchange in tackling undeclared work, France.
- Data exchange and data protection approach in Portugal.

3.1 Tools for cross-border data exchange

Member States use different tools for gathering, processing and transferring data for tackling undeclared work at national and cross-border level. These need to meet all the requirements and principles for data protection. Most of the existing data exchange for tackling undeclared work is concentrated between enforcement authorities on **national level** and on individual cases[9]. Data exchange at the **cross-border level** has been limited to ad hoc cooperation on individual cases[10].

The **Netherlands** has been one of the countries that have applied and piloted instruments for data exchange at national and cross border level. It has a well-developed **national system of cooperation and data exchange** in tackling undeclared work. It relies on two tools: (i) joint inspections teams (tax, social security, inspectorate, municipalities), which are approved by the Council of Ministers; and (ii) *Suwinet* services, which connects and allows the exchange of all the tax and social security data needed for tackling undeclared work. The services also allow the consultation and use of data of citizens (personal data) by public authorities.

At **cross-border level** the Netherlands has piloted with Belgium: (i) data exchange on micro level (individual cases) through joint actions on fraudulent temporary employment agencies, and (ii) data matching for identifying undeclared work cases based on social security data discrepancies between the two countries. There were important lessons learnt from both pilots, which other Member States and the EU could use in improving data exchange in the future.

At **micro level**, **in setting up joint actions** on fraudulent temporary employment agencies, both existing trust and understanding of the legal bases of the two countries played important roles. Yet, it is still important that the cooperating enforcement bodies invest sufficient time in road-mapping, or preparing the joint action plan. Very importantly, the existence of a sound national legal base and practices for data exchange as well allows for better and more efficient cooperation on cross-border cases. In this case, both countries relied on EU law (e.g. the posting and enforcement directives), on a bilateral treaty, and on the IMI module on posting of workers for the exchange of information across the border.

At **meso-level**, the Netherlands and Belgium tested **data matching between databases**. The overarching goal of the project was to check whether the use big data was feasible and whether it could help detect UDW. The objectives of the pilot included identifying Dutch persons in Belgian databases and vice versa; testing the connectivity between databases; identifying cases of undeclared work; and checking if the existing legal base is sufficient. The pilot involved personal data of about 10,000 people (names, date of birth, address), and data on social security income.

[9] Key conclusions from the Working group on 'Developing an IMI module for undeclared work, data sources and tools for inspectors' (23 May 2019, Brussels). Unpublished.
[10] European Platform tackling undeclared work, Follow up visit: Cross-border concerted and joint inspections, The Hague, 3 July 2019.

Box 3. Lessons learnt for the future use of big data cross-border exchange from the Netherland – Belgium pilot

The pilot exchange of access to whole databases between the Netherland and Belgium revealed some important insights, which other Member States and the EU could use, such as:

- Many **practical issues** were identified that need to be solved for data exchange to function automatically (e.g. small discrepancies between databases can hamper data exchange, such as the use of full first name in one database vs. the use of the first letter of the first name).
- At national level **different data bases must be combined** before moving on to cross-border level (e.g. registration of municipalities, data on income or posted workers).
- As many relevant actors as possible should be involved (inspectorates, social security, tax, municipalities). **Tax authorities** were not really involved but after evaluating the outcomes it became clear that they were much better equipped to deal with data exchange. They are more used to analysing databases and have treaties for exchange across borders, so they have more resources for such big-data assessments.
- Such data exchange **requires a solid and harmonised legal base** in all countries involved. That is why the Netherlands and Belgium have started preparing an extension of their legislation to have such big data exchange options better included.

Source: Presentation from Hans Van Weeren, International Coordinator, Inspectorate for Social Affairs and Employment, Ministry of Social Affairs and Employment, the Netherlands Seventh Plenary of the European Platform tackling undeclared work, 24-25 October 2019, Brussels.

France exchanges data across borders primarily on micro level (individual cases) and through the IMI. Its legal base defines undeclared work as illegal work, which provides its enforcement authorities with more options and possibilities to collect and share data within the GDPR requirements. In relation to this France relies on bilateral agreements with many countries, which ensure that the two countries' authorities: (i) are well aware of the underlying legal base differences, (ii) exchange information on sectors where high risks of undeclared work have been identified; and (iii) exchange information on ongoing joint inspections and actions. An important element of the French system for labour inspection and related data exchange is its **regional character**. France has one central Information Exchange Liaison Office, which operates through a national network with seven decentralised offices. Each of the decentralised offices ensures cooperation with the bordering regions or countries adjacent to France (Germany, Belgium, Spain, Italy and Luxembourg).

The decentralisation of cooperation and data exchange allows for greater efficiency and the handling of higher volumes of exchange without creating bottle-necks. However, when bilateral cooperation is very intensive, as in the case with Belgium for example, then regional offices have to resort to **non-IMI methods of exchange** (including secure e-mail) to ensure the fluidity and effectiveness of the process. For such non-IMI exchange to be feasible, there is a need for the two countries to have very high level of understanding of each other's legal base and have a high level of interoperability (in the specific case the two countries share a common language). In its bilateral cooperation with Portugal (signed agreement in 2017), France has introduced **the appointment of local correspondents** for data exchange in the six areas in which more than 80% of the Portuguese companies operate. This is meant to ease the exchange of data through more direct communication, including with the companies on the ground.

Portugal's data exchange related to tackling undeclared work is also more traditionally focused on the micro level (individual cases) and the use of bilateral agreements and IMI. The country has signed three such agreements: with Spain (2003), Belgium (2009), and

France (2017). In terms of the types of data exchanged Portugal has relied on company data (no personal data involved), data on work conditions and labour relations (which by law is the mandate of the labour inspectorate), and requests for information from other public administrations. The labour inspectorate has begun working towards developing clear written procedures for data exchange and the increase of the acceptability of data exchange and data protection rules among its employees.

3.2 Data protection challenges for cross-border data exchange

Enforcement bodies face different challenges when they exchange data on (i) micro level for individual cases and on (ii) meso level for risk assessment and profiling (exchange of whole (anonymised) datasets).

On **micro level with the exchange of case-related data** the two key existing exchange challenges are:

- Insufficient knowledge - of data protection rules, how to implement them and what can(not) be exchanged; and
- Lack of capacity - both human (DPOs) and technical (secure devices, encryption / transfer systems).

On the **meso level with the exchange of anonymised datasets** the challenges include:

- Introducing rules for anonymisation of data so that no data protection challenges appear;
- Lack of national datasets;
- Lack of dataset interoperability for merging datasets;
- Lack of human resource to integrate datasets;
- Lack of usefulness for inspections, as anonymisation does not allow risk profiling of specific companies or workers.

3.3 Measures to address data protection and data exchange challenges

Addressing the identified data exchange challenges requires different instruments and measures. These could build upon the tools currently available at European level that can ease cross-border data exchange, including: the **IMI system**, the **Electronic Exchange of Social Security Information**, the **interconnection** of central, commercial and company registers, etc. The participants at the thematic day have identified the following possible measures for enhancing data exchange:

- Addressing **micro level** (case-related) personal data exchange challenges:
  - Measures concerning insufficient knowledge of data protection rules, how to implement them and what can(not) be exchanged: training, advisory services and support. It is recommended that such measures are first piloted and then fine-tuned and mainstreamed.
  - Lack of capacity - human (DPOs) and technical (secure devices, encryption / transfer systems): Improved human and technological resources; pilots.
- Addressing **meso-level** (anonymised dataset exchanges) challenges:
  - Pilot studies of the experience in such data exchanges (they currently exist, among others, between: Estonia and Finland who have connected their public information exchange layers, though actual exchange of data has been limited to specific domains, on which there is agreement (e.g. population registration); the Netherlands and Belgium who have been exploring provision of direct access to each other's databases).

At the same time participants have also proposed the development of new tools for data exchange at the two levels, which Member States and the EU could strive to develop:

- Targeting **micro-level** data exchange:
  - New IMI module on undeclared work.
  - Handbooks on data exchange procedures and GDPR rules.
  - Mutual learning to share experience and build capacity.
  - Templates for BAs and MoUs for exchange of information.
  - Training of data protection officers.
  - Provision of generic data impact assessment methodology.
  - Support for secure transfer of data (creation of new systems, 'who's who' lists, summary of national legal bases, checklists, etc.).
  - **Joint action centre** during operational period/assistance programme/ learning events and seminars.
- Targeting **meso level** data exchange (whole databases):
  - Feasibility study on: dataset sharing; dataset collation; dataset interoperability; and data mining and analysis.
  - Staff exchanges to learn from the countries that have more advanced cross-border and national data exchange practices, such as Belgium, the Netherlands, France, etc.
- Targeting **macro-level** promotion of data exchange practices: campaigns to advertise outcomes of micro- and meso-level outcomes

4 ADDRESSING DATA PROTECTION MYTHS: EVOLUTION OF NATIONAL INSTITUTIONAL RESPONSES

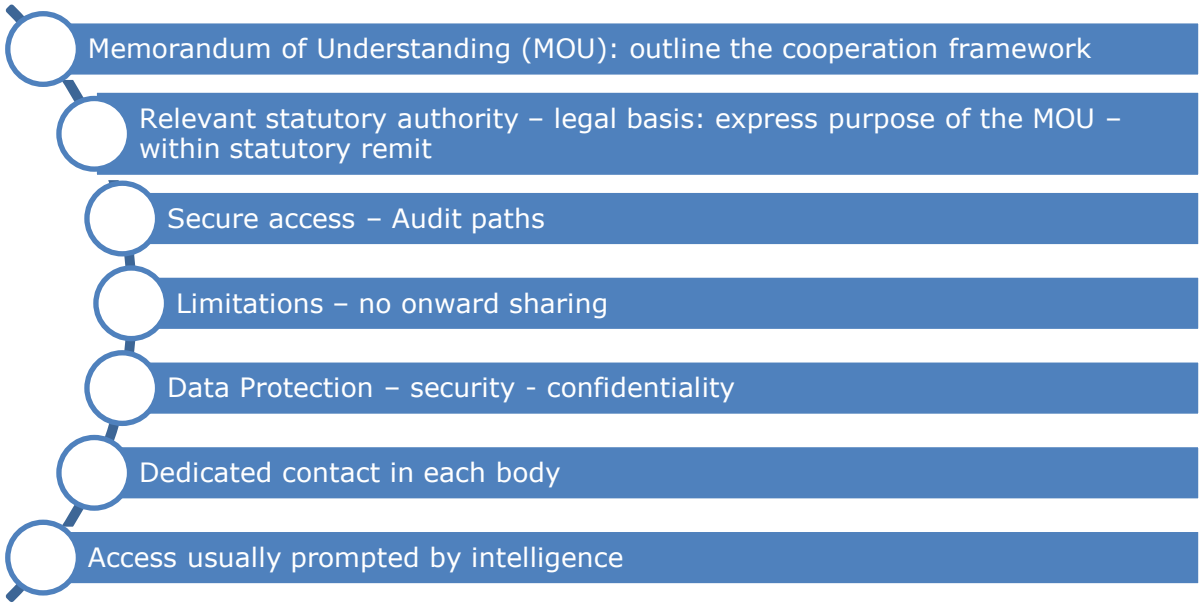
The second workshop of the Plenary thematic day focused on providing an overview of the evolution of data protection regimes in different Member States and 'demystifying' data protection regulations. There were three presentations, from Greece, Slovakia and Ireland, which showed each country's evolution path and current challenges of data protection and data exchange in tackling undeclared work.

The three case studies provided **different approaches to defining the public interest and the mandate of organisations** in tackling undeclared work, which provide the justification for data exchange and data protection. **Greece** has a definition of undeclared work in its law and of the powers of the institutions tasked for dealing with it. **Slovakia** has effectively copied the provisions of the GDPR into national law, which prescribes the cases, when the labour and social security authorities have rights to collect and exchange data. In **Ireland**, there is no definition of undeclared work but the laws and practice treat undeclared work as non-compliance, hence offence, which allows for more intensive data collection and data sharing among relevant authorities.

While having **a definition of undeclared work in the legislation** might help clarify public interest and official roles, it does not seem to be indispensable. Besides, authorities do seem to have more comprehensive data exchange practices if undeclared work is defined as a criminal offence. As criminal offences and roles in the criminal process tend to be well defined in legal terms, in such cases, data protection rules allow for a wider scope of exchange of data and authorities feel more secure about the applicable regulations. In particular, for cross-border information sharing there is a need for the two exchanging sides to be aware of whether the procedures are administrative or criminal as different data exchange rules apply.

In all three cases though authorities have **developed procedures and tools for exchanging data** on national level, trying to move from individual cases into more systemic (database) exchanges of data. In all three country-cases **data protection officers have been appointed** and they have developed the internal procedures for data exchange, as well as started making decisions on specific cases. For example, in Greece, for the first part of 2019 the DPO received some 100 requests for clarification and decision.

Figure 4. Protocols of exchange of data of the labour inspection (Workplace Relations Commission) in Ireland



Source: Presentation from Fran Power, Inspection and Enforcement Services, Workplace Relations Commission, Ireland, Seventh Plenary of the European Platform tackling undeclared work, 24-25 October 2019, Brussels.

It has become clear that different data protection and data exchange **cultures** have developed, including based on different interpretation of the GDPR and previously existing data protection rules. Changing such cultures requires experimenting, and practices and can be done within the existing GDPR regime. Ireland has presented an example of an evolutionary path, starting from a culture of secrecy, which then developed into a tax and social security data exchange, which has since been put into law. Ultimately, there is currently a general understanding that **data sharing in the public interest is doable**, provided data protection (GDPR) rules are abided by.

Greece updated its data protection legislation in 2019 to reflect the GDPR. The introduction of the GDPR has helped sensitise labour inspectors to the need of properly collecting, storing and disposing of data. Simultaneously, Greek authorities have sought to ensure **operability** between the databases of used by the Hellenic Labour Inspectorate (SEPE) and the Single Social Security Institution (EFKA). This has resulted in the development of different levels of access to the data contained in the ERGANI information system, as well as the introduction of more secure means of data transfer, such as password protection of files. In accordance with the GDPR requirements, the Ministry of Labour and Social Affairs and SEPE have appointed a data protection officer. The officer is responsible for monitoring the Ministry's compliance with GDPR, supporting and advising on its data protection obligations, and acting as a contact point for data subjects and the relevant supervisory authority. The Greek authorities have outlined three **key data protection challenges** they face: (a) keeping data safe; (b) justifying data exchange; and (c) properly notifying the data subject. These have been addressed by increasing the number of seminars and knowledge exchanges, upgrading and updating regularly information technology systems and hardware, enduring different levels of authorised access to databases, etc.

Slovakia, similarly to Greece, also updated its data protection legislation with the adoption of the GDPR. The Slovak laws on labour inspection and on illegal work as well as illegal employment state that the competent authorities are allowed to handle workers' data even without their consent. However, the data can be transferred to another country only if there is a legal base for the transfer. Currently, the legal base **only allows data to be transmitted to another Member State through the IMI**. The Slovak inspectorate exchanges data nationally both through databases and through individual requests. There are some 31 different databases, to which the inspectorate has access (e.g. database of socially insured, database of posted workers, Labour Protection Database, database of illegaly emloyed, database of issued A1 forms, etc.).

The Slovak inspectorate's most important data exchanges are with the Slovak Insurance Agency via access to the **database of the socially insured**. All labour inspectors have password protected access to it on the basis of personal identification cards (GRID card). Conditions of access to the database are regulated by law and mutual agreements between the National Labour Inspectorate and the Slovak Insurance Agency. In June 2019 the inspectorate and the agency developed **a tool to detect instances of under-declared work** in connection with social security deductions. Access to the tool will happen through the GRID cards. Currently no data exchange is possible between the inspectorate and Slovak tax authorities as tax secrecy applies. But there are plans for such exchange to be launched soon in connection with preparation of analytical tools needed for surveys and investigation of instances of undeclared work.

The lack of legal base, very strict application of the 'limitation of purpose' principle and lack of appropriate tools for data exchange have been some of the **barriers** the Slovak labour inspectorate has encountered in data exchange.

The workshop has identified **three general challenges** in relation to data exchange and data protection: (i) **legal** (in particular in cross-border exchanges, where there is no existing legal database; generally there is uncertainty and risk aversion to try to test the boundaries of what is legally allowed; oftentimes this is not done due to the lack of technical capabilities); (ii) **technical** (lack of technical capabilities to exchange data securely and in line with all good guidelines); (iii) **cultural** – lack of vision and leadership to strive for more data exchange in pursuit of the public interest.

Accordingly, there have been several types of measures most often proposed to be developed at **EU level** to help improve data exchange and data protection at the cross-border level:

- Developing a multilateral legal base for data exchange.
- Enabling data exchange through better knowledge of existing national practices and procedures through an EU wide database of national data exchange characteristics.
- Providing training and capacity building for cooperation between DPOs and enforcement bodies' personnel.
- Developing new or enhancing existing tools for the exchange of data that provide guaranteed level of data protection (such as IMI).
- Provide common certification of information systems used by relevant enforcement bodies from multiple Member States.

5 CONCLUSIONS AND THE WAY FORWARD

The Plenary thematic day confirmed the findings of the input paper and the data protection and data exchange paper prepared for the Platform.

Several important **conclusions** can be drawn from the discussions:

- **Cross border data exchange at the micro (individual case) level is already happening**, through the IMI and with the help of bilateral agreements. However, the evidence in relation to cross-border **joint inspections and related data**

exchange shows that they **are infrequent**. The exchanging of registers and databases (anonymised) is also possible but so far is only limited to pilots, such as the one between Belgium and the Netherlands.

- Currently, the **IMI is the most frequently used tool for cross-border data exchange on tackling undeclared work.** However, it is only used for solving individual cases, not for the exchange of whole databases. In addition, the IMI posting module is being used de facto to address undeclared work cases, including some that might fall outside of the posting field. As the IMI guarantees evidence-grade level data exchange between enforcement bodies, it seems reasonable to consider **developing a specific module for undeclared work**[11].
- One of the discussions that emerged from the thematic day is whether classifying **undeclared work or aspects of it as criminal offence** could enable more efficient data exchange. Such experience already exists in Member States (e.g. France, Belgium). This could also allow better harmonisation between administrative and criminal procedures of exchange of data in tackling undeclared work.
- At cross-border level there is currently **insufficient knowledge** and **lack of capacity** for data exchange. This is particularly challenging when the exchange of whole databases is being used for risk assessment or strategic planning.
- The different case studies for data exchange during the thematic day have demonstrated that **at national level, the exchange of data is less challenging**, provided the respective authorities have the legal base and the mandate to do it. Countries like Spain, Belgium, Ireland, etc. have developed diverse solutions for inter-institutional data-exchange in different legal contexts. **Such experiences could be transferred to cross-border level** given sufficient resource, cooperation and capacity to do so, and the Platform instruments for experience and knowledge exchange could help in this regard (staff exchange, Mutual Assistance Projects, toolkits, etc.).
- In this regard, ELA has risk analysis as one of its core tasks, which could help increase knowledge and capacity for cross-border data exchange. This could complement what Member States are already doing in the area of undeclared work. ELA could also aid cross-border data exchange.

[11] See Key conclusions from the Working group on 'Developing an IMI module for undeclared work, data sources and tools for inspectors' (23 May 2019, Brussels). Unpublished.