

# European Labour Authority

## **Secure exchange of information**

1

Trainer

# Introduction of the trainer



Nora Sajbidor  
Manager | PwC

Nora is a senior **legal counsel** with **more than 7 years of professional experience**. She specializes *inter alia* in **data protection** law and is experienced in giving presentations and providing trainings on data protection matters to diverse audiences.

# Agenda

1

Welcome/Introduction of the trainer

2

Train the Trainer Model

3

GDPR and data protection

4

Data exchange systems: IMI, EESSI

5

Use case #4 - IMI national practices

6

Discussion and closing remarks of the day

2

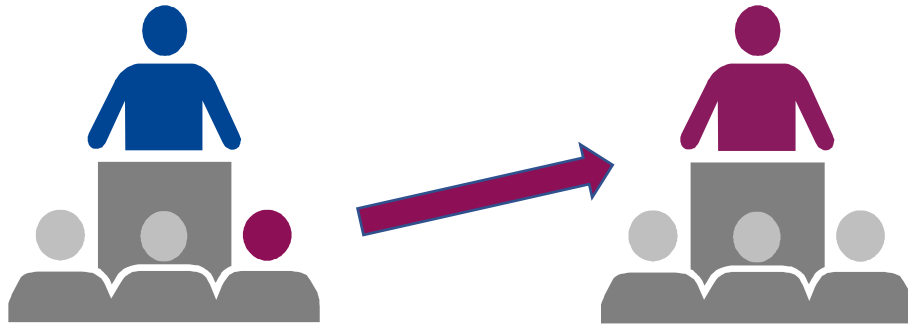
Training model

# Train the Trainer Model

- ✓ The Train the trainer model is **widely used training strategy**
- ✓ Subject-matter expert is trained to **become a training instructor**
- ✓ The method offers distinct **advantages** over other training models because trainees typically **learn faster and retain the information better** than in other teaching models
- ✓ **Spillover effect** of training - it's enable the education of a larger number of participants



# Train the trainer model



The **trainer**, a subject-matter expert, **trains other participants** from Member States and simultaneously **teaches** them **how to train others** in the secure exchange of information.

All participants will be encouraged to **conduct similar trainings** for other stakeholders (**Inspectors and Social partners**) in their respective Member States.

## HOW?


- The participant will **receive material** that will use during the presentation in Member State.
- The participant will use **own remarks** from today's training.

## WHAT materials?

1. **Presentation with notes** for the trainer.

### What is IMI?

- IMI = **Internal Market Information** system
- An online tool that **facilitates information exchange between public authorities** involved in the practical implementation of EU law
- Used by authorities across the EU and in Iceland, Lichtenstein and Norway
- Maintained by the **European Commission**
- Regulated by the **IMI Regulation** (No 1024/2012)



The aim of IMI system is to help EU countries, Iceland, Lichtenstein and Norway meet their mutual assistance obligations in an efficient and effective manner at minimum resource cost and without building a separate information system to support each individual legal instrument.

The tool was developed by the European Commission in cooperation with Member States. Today the Commission hosts and maintains the system.

**Facts and figures:**  
The first information exchanges took place in 2008. The total number of all IMI exchanges exceeds 207 000.

The volumes of IMI information requests have increased from 30 per month in 2008 to more than 1500 per month in 2019.

There are now more than 12 000 registered authorities with over 35 000 registered users.

The legal basis for IMI is the IMI Regulation adopted in 2012. The IMI Regulation sets out the scope of IMI, the roles and responsibilities of the different actors, and rules for handling personal data.

3

GDPR and data  
protection



# What is the GDPR?



An EU directive that governs how companies and organizations process personal data



An EU regulation that governs how companies and organizations process personal data



An EU regulation that governs how companies and organizations process data, including personal data

# 3.1 GDPR in a nutshell

# Introduction

- GDPR = **General Data Protection Regulation**
- As an EU Regulation (Regulation (EU) 2016/679) the GDPR is **directly applicable in each Member State**
- Introduced a **uniform legal framework for the processing and protection of personal data**
- Is supplemented by **national data protection laws of Member States**

# Scope of application

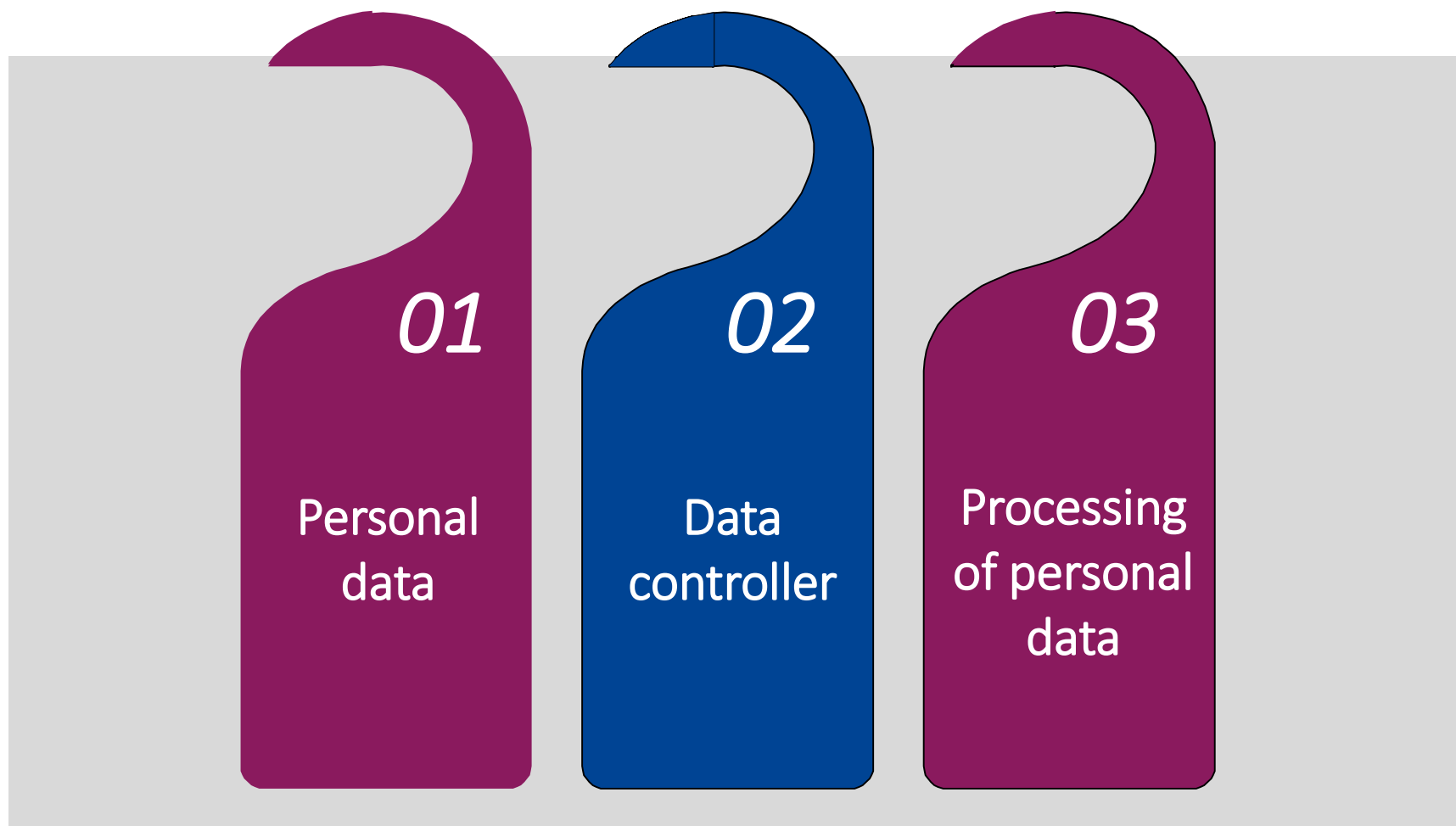


GDPR applies to processing of personal data by Member States **in the course of an activity within the scope of EU law** - processing of personal data **by national authorities of Member States in the context of EU labour mobility issues (including concerted and joint inspections)** will be governed by the GDPR



GDPR **does not apply to** processing of personal data by **EU institutions, bodies, offices and agencies** - such personal data processing is governed by **Regulation (EU) 2018/1725**, including the processing of personal data **by the ELA in the context of concerted and joint inspections**

# Basic data protection concepts



# Personal Data

**Personal data** is any information that relates to an *identified natural person\** or *from which a natural person may be identified*. This includes:

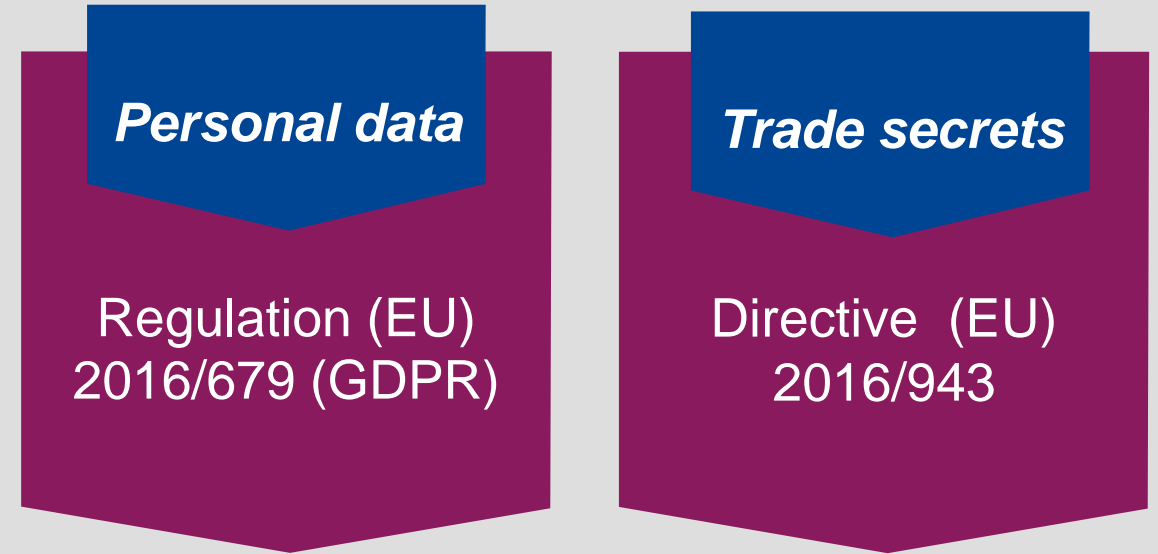
<i>Name</i>	<i>Languages spoken</i>	<i>Racial or ethnic origin</i>
<i>Gender</i>	<i>National ID numbers</i>	<i>Political opinions</i>
<i>Age and date of birth</i>	<i>Passport no.</i>	<i>Religion</i>
<i>Marital status</i>	<i>Driver's license no.</i>	<i>Trade-union membership</i>
<i>Addresses, phone numbers</i>	<i>Identity verification info</i>	<i>Genetic /Biometric data</i>
<i>Employer</i>	<i>Email address</i>	<i>Medical records and other data relating to health</i>
<i>Citizenship</i>	<i>Location data</i>	<i>Sexual orientation</i>
<i>Veteran status</i>	<i>IP address</i>	<i>Disabled status</i>
<i>Photograph</i>	<i>Other online identifiers</i>	

\* A 'natural person' is an individual, not a legal person (company/corporation).

# Personal data vs trade secrets

- **Personal data** and **trade secrets** are two different concepts
- **Trade secret** means information which:
  - ✓ is secret (is not public nor readily accessible)
  - ✓ has commercial value because it is secret; and
  - ✓ reasonable steps have been taken by the person lawfully controlling the information to keep it secret

They are **protected by different EU legislation**:



Distinction between personal data and trade secrets is important so that **the relevant legal framework** is followed

ELA will provide its support to the Member States participating in concerted or joint inspections **in full respect of confidentiality requirements**

# Data controller

## ***Data controller***

Determines the means and purposes of data processing (the 'why' and the 'how')



# Processing of personal data

Means any operation performed on personal data, such as:

- Collection
- Downloading
- Recording
- Organization
- Structuring
- Storage
- Adaptation or alteration
- Retrieval
- Use
- Disclosure or otherwise making available
- Combination
- Blocking
- Erasure
- Destruction



# Principles of data protection (1/4)

## The GDPR sets out 7 principles

1 Lawfulness, fairness and transparency

2 Purpose limitation

3 Data minimisation

4 Accuracy

5 Storage limitation

6 Integrity and confidentiality (security)

7 Accountability

Compliance with these principles of data protection is **key for compliance with the GDPR**

# Principles of data protection (2/4)



## Lawfulness, fairness and transparency

personal data must be processed lawfully, fairly and in a transparent manner in relation to the individuals whose personal data is being processed:

- Lawfulness** → A lawful basis for the processing of personal data (e.g. processing is necessary in the exercise of official authority vested in the data controller)
- Fairness** → Fair and reasonably expected use of personal data
- Transparency** → Open communication on the personal data processing towards the individuals whose personal data is being processed (e.g. posted workers)

# Principles of data protection (3/4)



## Purpose limitation

personal data can only be **collected for specified, explicit and legitimate purposes** (e.g. conducting an inspection with the aim to detect non-compliance with legislation on posting of workers) and can not be further processed in a manner that is incompatible with those purposes



## Data minimization

personal data that is processed must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

# Principles of data protection (4/4)



## **Accuracy**

personal data must be kept accurate and up-to-date and if it is not it must be corrected or erased



## **Storage limitation**

personal data can be stored only as long as it is needed for lawful processing



## **Integrity and confidentiality (security)**

appropriate security measures should be in place to protect the personal data (e.g. sharing of personal data via the IMI system)

# Rights of data subjects

The GDPR provides a number of rights to individuals whose personal data is processed. In the context of inspections these are the most relevant rights:



1 Right to be informed

2 Right of access

3 Right to rectification

4 Right to erasure (right to be forgotten)

# Consequences of non-compliance

Consequences of non-compliance with the GDPR by public authorities include:



Fines

Claims for damages

Harm to reputation

Whether fines may be imposed on public authorities and in what amounts depends on national legislation\*:

- In some Member States administrative **fines cannot be imposed on public authorities** (e.g. Austria, Belgium, Germany)
- In some states the **amount of the administrative fines is lower** compared to the GDPR (e.g. Czech republic, Poland, Slovenia, Sweden)
- In some states the **administrative fines under the GDPR apply** (e.g. Italy, Latvia, the Netherlands)

source: <https://www.whitecase.com/publications/article/gdpr-guide-national-implementation>

# 3.2 Data protection in the context of CJIs

# Introduction

**Principles of data protection** must be observed in each phase of a concerted or joint inspection:



**Planning**



**Implementing**



**Following-up**

Participating Member States and the ELA must ensure that the processing of personal data carried out during CJs is **compliant with the GDPR and the national data protection legislation** of each participating Member State

- **Lawfulness, fairness and transparency**
- **Purpose limitation**
- **Data minimization**
- **Integrity and confidentiality (security)**
- **Accuracy**
- **Storage limitation**
- **Accountability**



# Planning the CJI (1/2)

The initiating Member State **identifies a case** that should be the subject-matter of a CJI, **identifies other stakeholders and shares information on the case**

## What needs to be verified?

- Whether communication with the other stakeholders require sharing of personal data
- That there a legal basis for processing of such personal data
- That the extent of the shared personal data is adequate, limited to what is necessary and that the data is shared in a secure way

The requesting Member State(s) **complete the Case description** template

## What needs to be verified?

- What personal data needs to be included to provide a relevant description of the case
- That there a legal basis for processing of such personal data
- That the extent of the shared personal data is adequate, limited to what is necessary and that the data is provided in a secure way

# Planning the CJI (2/2)

- Member States and ELA complete and sign **the Model Agreement**
- Member States and ELA finalize **the Inspection Plan which is an annex to the model Agreement**

## What needs to be determined?

- What information, documents and evidence containing personal data is to be obtained at the inspected entities
- What personal data will be collected by means of the questionnaires and other documents during the inspection
- Who will be the responsible persons for data exchange and which channels will be used for data exchange

# Implementing a CJI (1/3)

During the **on-site-stage of CJIs** the inspectors from participating Member States **follow the instructions set out in the Inspection Plan**. CJIs shall be carried out in accordance with the **law or practice of the Member States in which the inspections take place**.

## Matters to keep in mind:

- Using questionnaires and forms that are compliant with the law of the Member States in which the inspections take place
- During interviews asking questions allowed under the law of the Member States in which the inspections take place
- Collecting documents or other evidence containing personal data and taking photos or making video/voice recordings to the extent allowed under the law of the Member States in which the inspections take place
- Providing information on processing of personal data (Articles 13 and 14 of the GDPR) in accordance with the law of the Member States in which the inspections take place

# Implementing a CJI (2/3)

After the on-site stage the **collected data will be** analyzed and **shared** between Member States and possibly also with other authorities and bodies. These activities must be carried out in accordance with **the law or practice of the Member States concerned**.

## Matters to keep in mind:

- Verifying that each data exchange involving personal data has a valid legal basis
- Providing only personal data that is relevant, adequate and limited to what is necessary to achieve the sought purpose
- Confirming that data subjects have been informed about the recipients of their personal data in accordance with the law or practice of the Member State concerned
- Using secure and data protection compliant channels for data exchange

# Implementing a CJI (3/3)

The **Post Inspection Report** will be completed by the inspection coordinator.

## Matters to keep in mind:

- Including personal data in the Post Inspection Report is not a requirement
- Including personal data in the Post Inspection Report is subject to the key data protection principles (in particular personal data can be included only if there is a lawful basis to do so, only to the extent adequate and necessary) and to the law of the Member State concerned

# Following up a CJI

After completion of a CJI, key findings are communicated:

- Externally, to inform other authorities, including those in other Member States
- Internally, to share results and lessons learnt with colleagues

Results of a CJI can also be shared widely with the public.

## Matters to keep in mind:

- Including personal data in the communication will probably not be necessary
- If processing of personal data takes place, it must be compliant with the data protection principles and the law of the Member State concerned

15 minutes  
coffee break



# 4

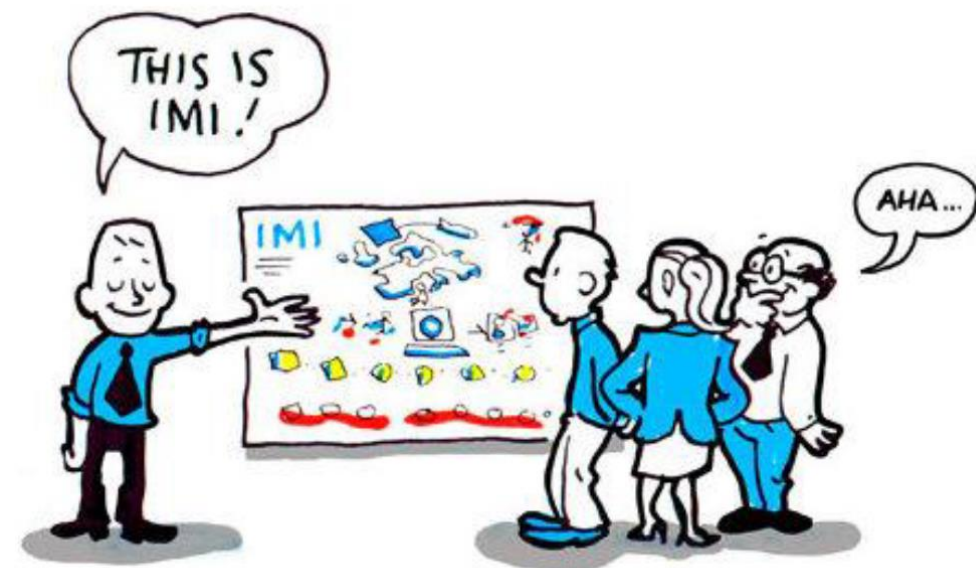
Data exchange  
systems: IMI,  
EESSI



# 4.1 Introduction to IMI

# What is IMI?

- IMI = **Internal Market Information** system
- An online tool that **facilitates information exchange between public authorities** involved in the practical implementation of EU law
- Used by authorities across the EU and in Iceland, Lichtenstein and Norway
- Maintained by the **European Commission**
- Regulated by the **IMI Regulation** (No 1024/2012)



# What areas are covered by IMI

Currently **18 different policy areas**, including:

- Professional qualifications
- Services
- **Posting of workers**
- Cash-in-transit
- Patients' rights
- SOLVIT
- E-commerce
- Train-driving licences
- Public procurement

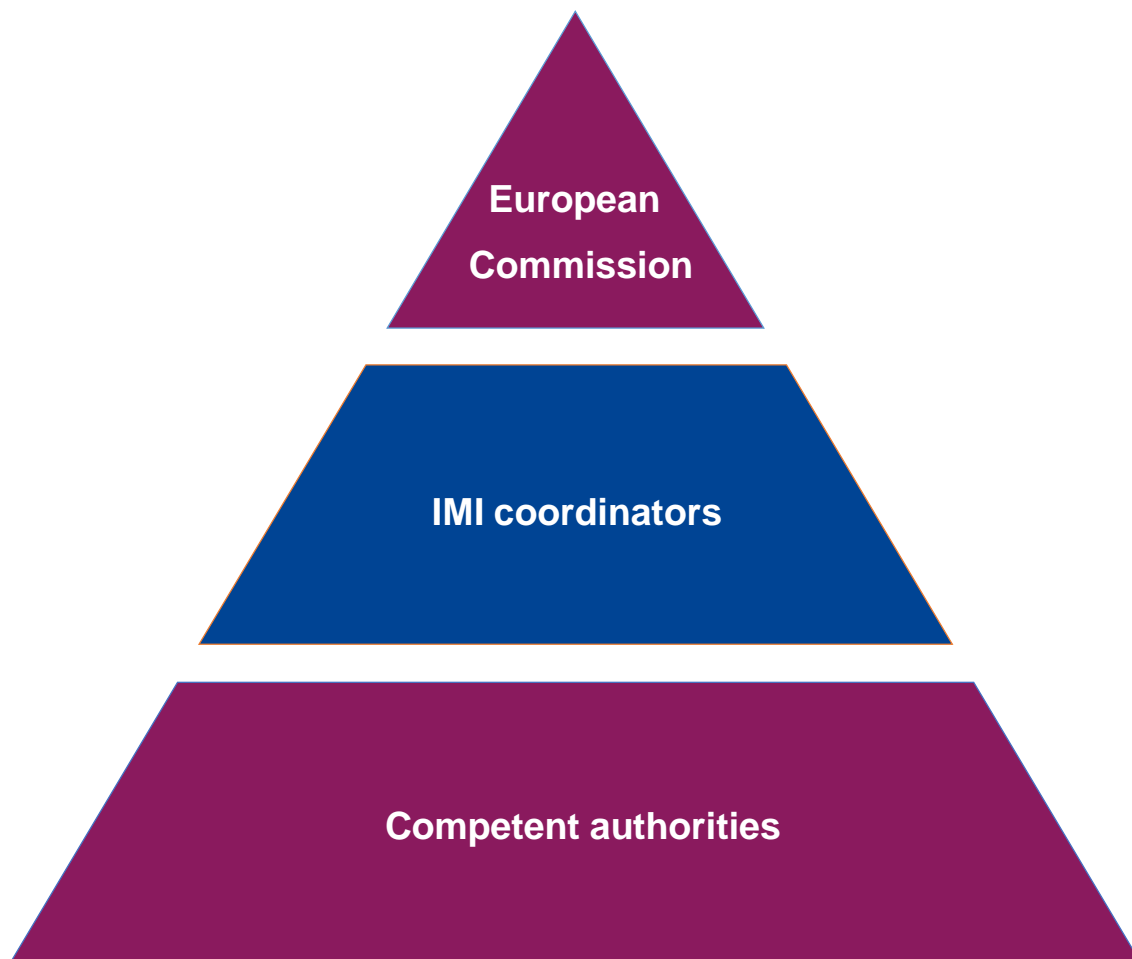


# What are the benefits of IMI?

- Helps authorities **identify their counterparts** in other countries and **communicate efficiently**
- **Secure and data protection friendly**
- **A multilingual tool:** available in all official EU languages
- **Overcomes language barriers:** standardised question/answer sets; automated translation is available for free text



# Who is involved in IMI?



The Commission **hosts and maintains the system**, runs a central helpdesk to assist Member States and is responsible for the translations in the system.

Each state has one national IMI coordinator, which **registers** the competent **authorities**, **manages access** to different modules and **provides support and training** to IMI actors.

Authorities tasked with applying EU single market legislation **exchange and share information via IMI**.

# 4.2 Data protection in IMI

# IMI and data protection in general

- Provides **a clear framework** for what information can be exchanged, with whom and under what circumstances
- Offers a **higher level of security** than regular mail, telephone, fax or unencrypted e-mail
- **Facilitates handling of data subjects' requests** for exercise of their rights under data protection legislation



# Access to personal data in IMI

- **Only registered IMI actors and users** have access to IMI
- Access to personal data on a **need-to-know basis**: IMI actors can only access personal data that is part of the information exchange that they are involved in;
- Every **data exchange is recorded in IMI**, IMI users who have handled an information exchange are traceable





# Retention of personal data

- Any **personal data** processed in IMI **is blocked** as a general rule **no later than 6 months** after the formal closure of the administrative cooperation procedure
- Blocked personal data may be processed, with the exception of storage, only for purposes of proof of an information exchange by means of IMI
- Blocked personal data will be **automatically deleted** in IMI 3 years **after** the formal closure of the administrative cooperation procedure



# Responsibility for personal data in IMI

Responsibility for personal data protection and security is shared between the IMI actors

## *European Commission is responsible for:*

- Ensuring the security of the IT infrastructure
- Collection, storage and deletion of personal data of IMI users
- Storage, blocking, deletion, and retrieval of personal data of persons who are the subject of an information exchange

## *Each competent authority and IMI coordinator:*

- Is a data controller and therefore is responsible for its own data processing activities
- Must ensure that data subjects can exercise their rights under data protection legislation (right to information about processing of their personal data, right of access, correction and deletion)

# 4.3 Information exchange in IMI in the area of Posting of Workers

# Posting of Workers in IMI

Pilot project launched in 2011

Usage formalised with the Enforcement Directive (2014/67/EU)

Latest update in July 2020 in the context of the revision of the Posting of Workers Directive

## Article 21(1) of the Enforcement Directive:

The **administrative cooperation and mutual assistance** between the competent authorities of the Member States provided for in

- Articles 6 and 7,
- Article 10(3),
- Articles 14 to 18

shall be **implemented through the Internal Market Information System (IMI)**

# How is data exchanged in IMI

IMI offers these types of information exchanges in the area of Posting of Workers:



“One-to-one” exchanges between two competent authorities.



“One-to-many” exchanges where MS can share information with other MS and/or the Commission.

# Posting of Workers

The mutual assistance requirements under the Posting of Workers Directive and the Enforcement Directive have been implemented in IMI through 4 modules:



1

Posting of Workers Information Request

2

Communication of Irregularities

3

Request to notify a decision imposing a penalty and/or fine

4

Requests to recover a penalty and/or fine

# Posting of Workers Information Request

The Request module is the most frequently used module for administrative cooperation and currently has 5 request forms:

1

Urgent request

2

Request concerning a posting

3

Request concerning Health and Safety

4

Request concerning Working Conditions

5

Request to send documents to a service provider

# Common structure for an information request

## Posting of Workers Information Request

1

Summary

2

Service Provider details (mandatory)

3

Posted Worker(s) details (optional)

4

Additional relevant information (some forms)

5

Questions or request

6

Comments and attachments





## Menu



Dashboard

Requests - Old forms (PQ, PR, SD, PP, ...)

Archived Requests

Requests - (CPC, EJM, PD, GDPR, PoW, ...)

Search all forms

Search by form

Create request

Notifications

Authorities

Session Log

My reports

My translations

Change my password

Logout

## Dashboard

Refresh

## Requests - (CPC, EJM, PD, GDPR, PoW, CO)

Summary of requests, which may require an action on your part

[Draft Requests](#) 25

Rec

PW - Posting of workers - request for information concerning a posting

PW - Posting of workers - request for information concerning health and safety

PW - Posting of workers - request for information concerning working conditions

PW - Request to send documents to a service provider

PW - Urgent request concerning establishment

Uniform Instrument - Request to notify a decision

Uniform Instrument - Request to recover a penalty and/or fine

## Notifications

Summary of notifications which may require an action on your part

[Draft notifications](#) 3

**Request summary**

Service provider

Questions and Answers

Messages and attachments

Management information

**Entry number** 10716      **Module** Posting of Workers - Information Request - PW - Urgent request concerning establishment      **Status** Draft  
**From** Hungary - HUA00 - ex 500 HU-NIMIC - Test's X      **Due date**  
**To** Cyprus - A870P NIMIC CY      **Date sent**

Request

**Urgent request for information concerning the establishment of a posting company**

**Confirmation** • This is an urgent request in accordance with Directive 2014/67/EU Article 6 (a)

**Reason for the urgency** Information required to .....

Dates

**Article 6 (a) of Directive 2014/67/EU stipulates that urgent requests shall be answered as soon as possible and within a maximum of 2 working days.**

**Number of calendar days in which a reply is required** 4

Select the responding authority

Informal title	Name	Country
A870P NIMIC CY	A870P NIMIC CY	Cyprus

Request summary

**Service provider**

Questions and Answers

Messages and attachments

Management information

#### Service provider details

<b>Type of service provider</b>	Other legal entity
<b>Company/Trading name</b>	Best traders
<b>Does the company have other trading name(s)</b>	No
<b>Legal form of the company</b>	(UK) Private Limited Company, LTD

#### Service sector

<b>Service activities</b>	<ul style="list-style-type: none"> <li>• Construction work</li> <li>• Construction-related services</li> </ul>
<b>NACE reference number(s) of the service sector(s)</b>	

#### Address

<b>Address of the service provider</b>	Unknown
--	---------

#### Contact details

<b>E-mail address</b>	
<b>Telephone number</b>	

#### Identification

<b>TAX/VAT number</b>	Known
<b>Tax/VAT</b>	CY1010

Request summary

Service provider

Questions and Answers

Messages and attachments

Management information

## Questions

Click on the questions to see further details, comment and answer fields. The fields are only editable if a question is selected in the request

*The recipient must provide an answer for each question*

### Questions

[U001] Is the service provider lawfully established in your Member State?

Question comments

Answer

Detailed answer

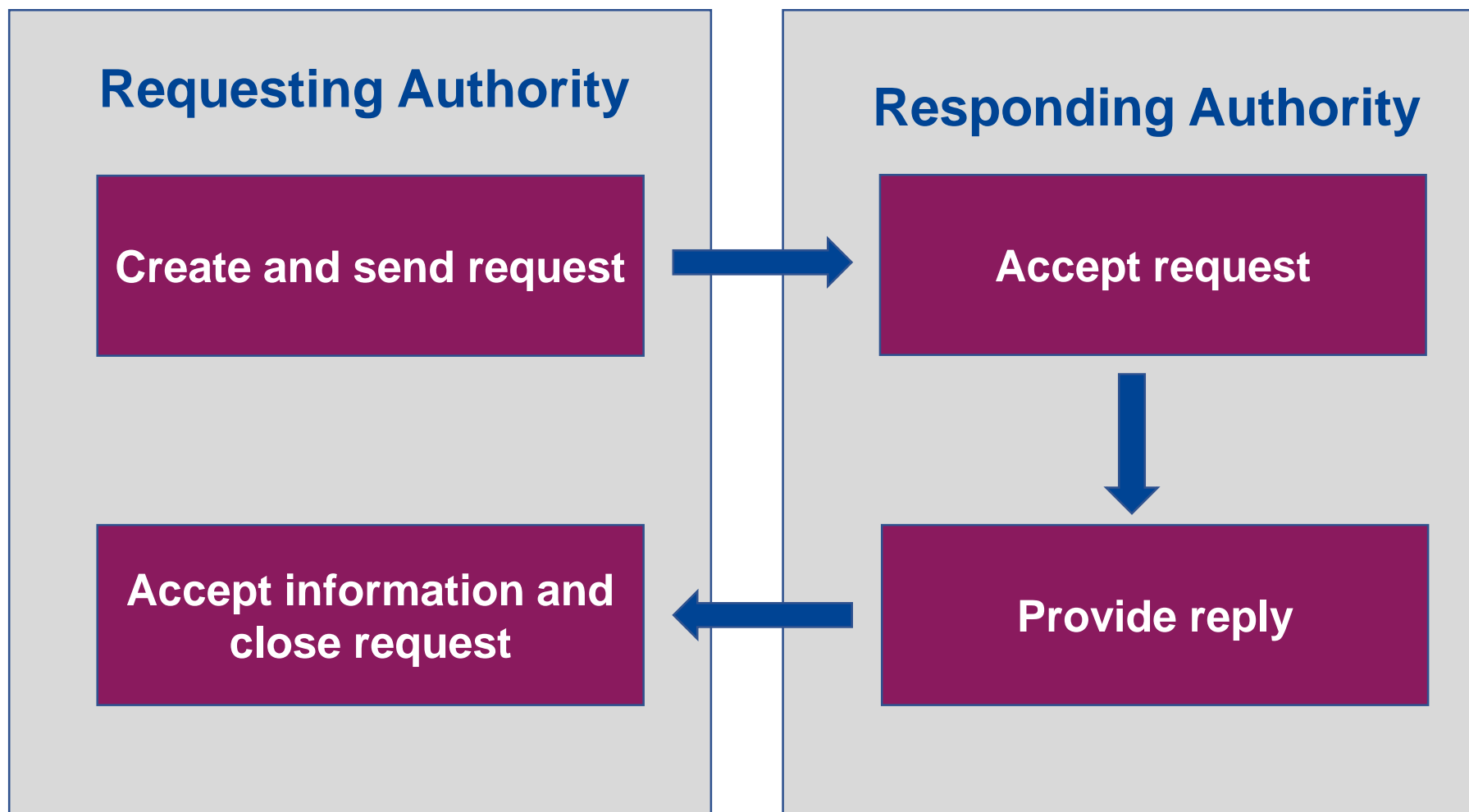
[U004] Does the service provider perform its substantial business activity in your Member State?

Question comments

Answer

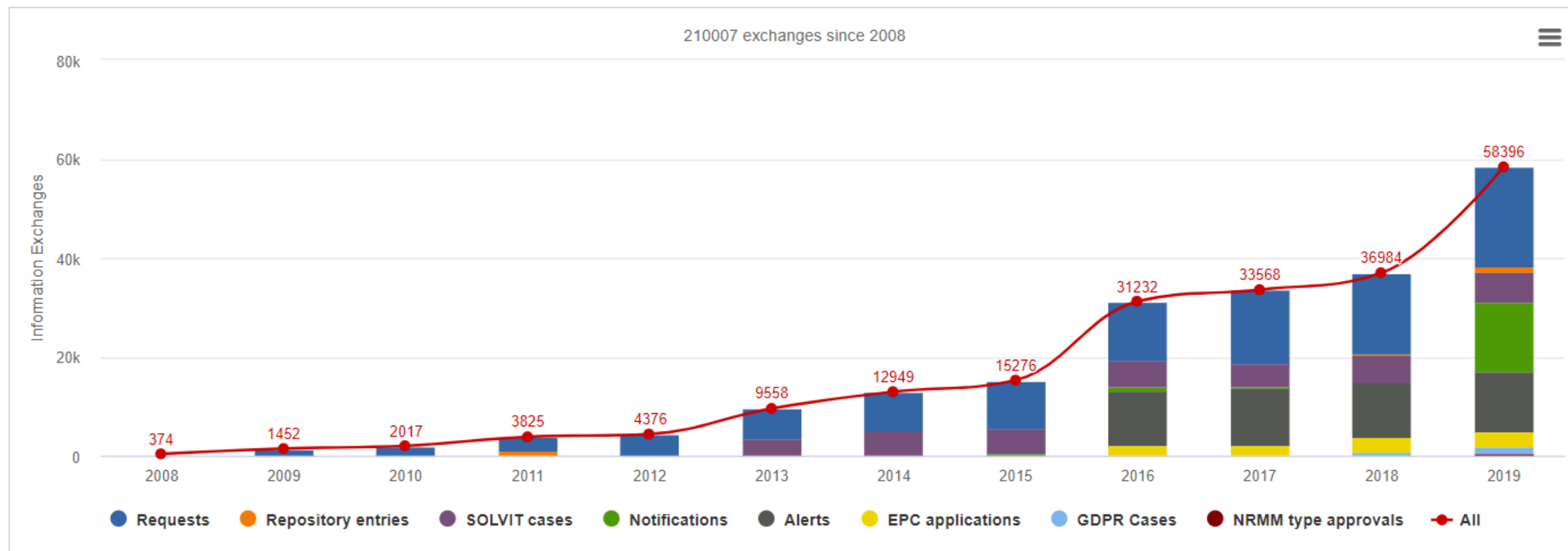
Detailed answer

# The request lifecycle

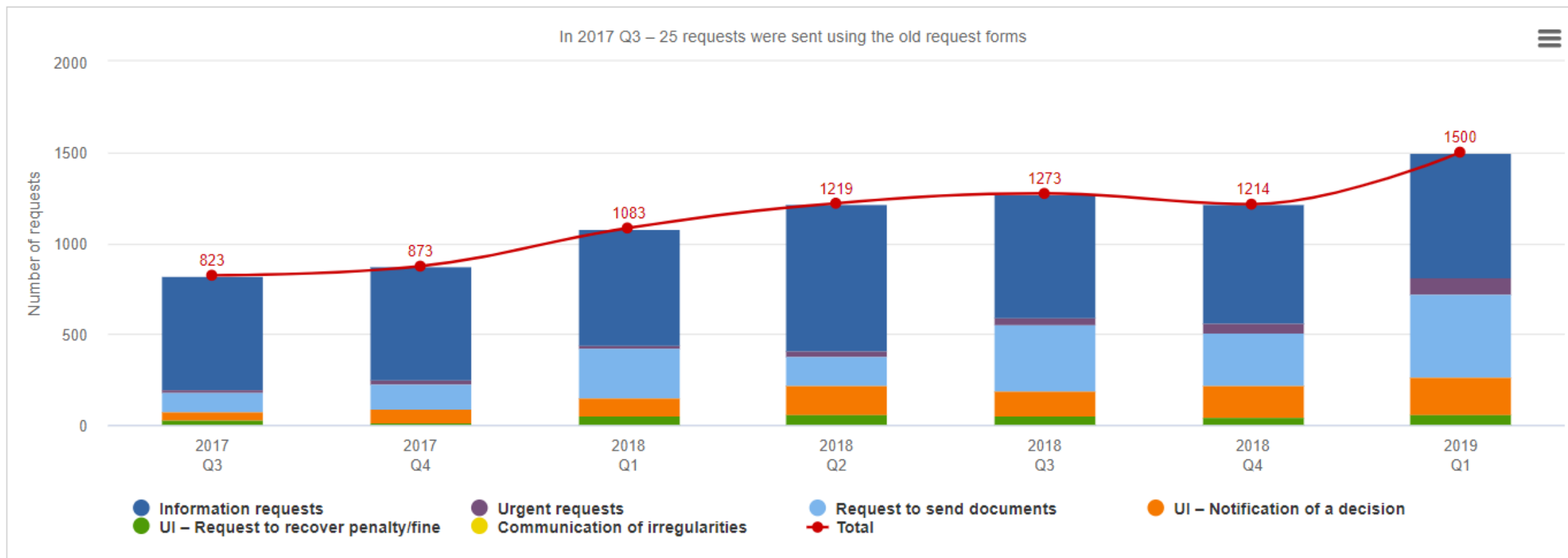


# 4.4 Statistics on the use of IMI

# All information exchanges in IMI, 2008-2019

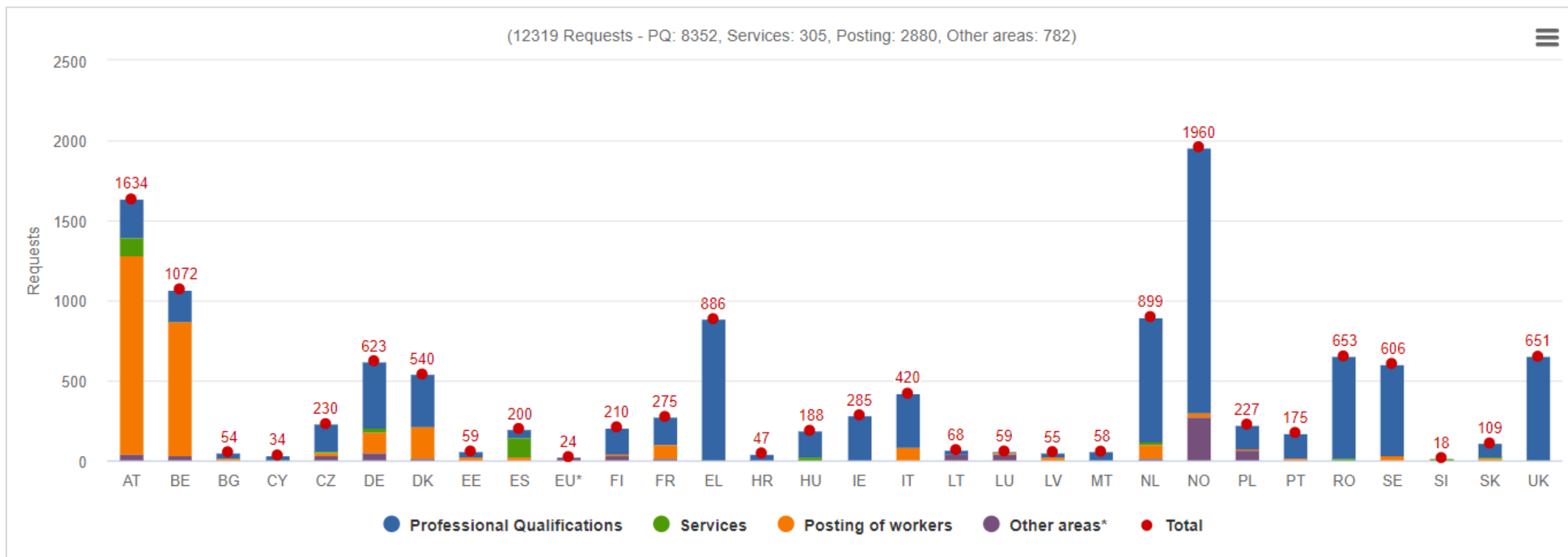


# Number of posting information exchanges per type Q3 2017 – Q1 2019

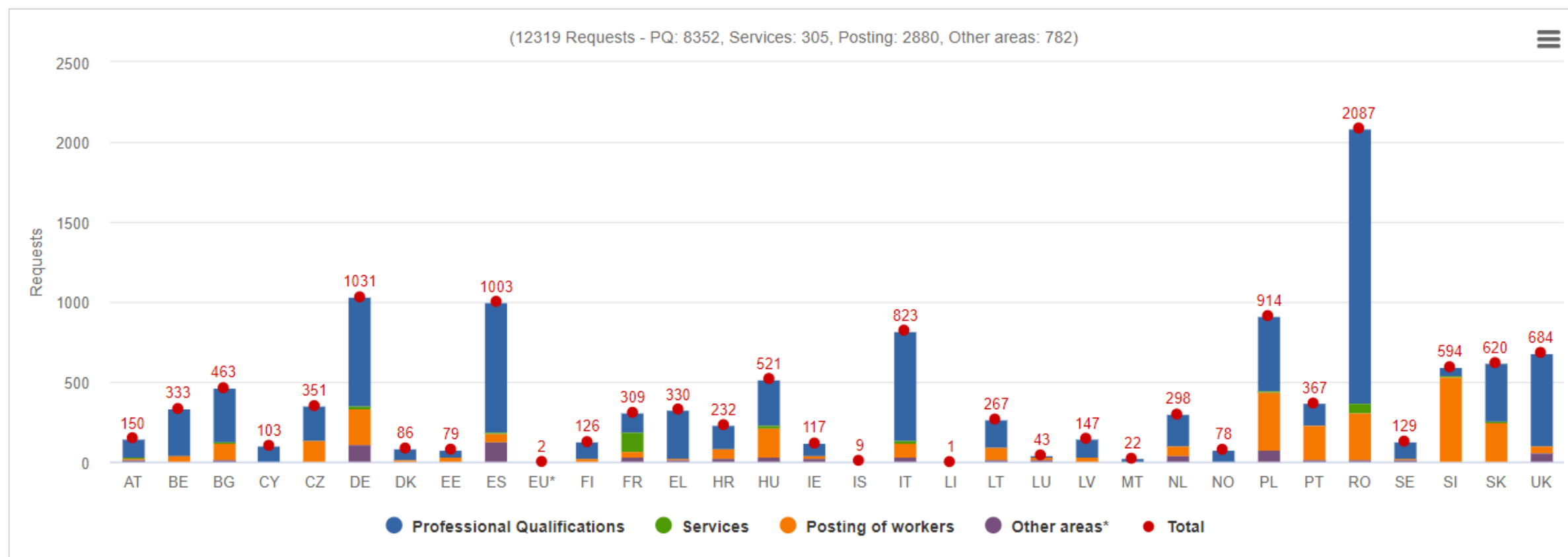




# IMI requests in 2020 by sending Member State (Q1 – Q3)



# IMI requests in 2020 by recipient Member State (Q1 – Q3)



4.5 EESSI

# What is EESSI?

- EESSI = **Electronic Exchange of Social Security Information**
- An IT system that **facilitates information exchange between social security institutions**
- Available to authorities in the EU, Iceland, Norway, Liechtenstein and Switzerland
- **First exchange of information** relating to a concrete case took place in **January 2019**

# What are the benefits of EESSI?

- ✓ Allows for **faster and more efficient information exchanges** between social security institutions in **8 branches of social security coordination**
- ✓ **Optimizes case handling** by means of standard electronic procedures
- ✓ Improves **multilingual communication**
- ✓ Enables **secure handling of personal data**

5

Use case - IMI  
national practices

# 6

Discussion and  
closing remarks of  
the day