European
Commission

The Internal Market Information (IMI) System

User handbook

Update 2012

Internal Market
and Services

EN

The Internal Market
Information (IMI) System

User handbook

Update 2012

Europe Direct is a service to help you find answers
to your questions about the European Union.

Freephone number (*):

00 800 6 7 8 9 10 11

(*) Certain mobile telephone operators do not allow access to 00 800 numbers or these calls may be billed.

More information on the European Union is available on the Internet (http://europa.eu).

Cataloguing data can be found at the end of this publication.

Luxembourg: Publications Office of the European Union, 2012

ISBN 978-92-79-26040-7
doi: 10.2780/75733

Table of Contents

1. Introduction

Welcome to the Internal Market Information (IMI) system.

IMI is a secure online tool that allows **national, regional and local authorities to communicate** quickly and easily with their counterparts abroad.

Whether you are already registered as an IMI user or about to register, this document is for you. It starts out by giving a **general introduction** on what IMI is and how it works. Then it explains **all the important IMI functionality** and how to use it. Not all functionality will be relevant to your work. As IMI is built in a **modular way**, each function works independently. Therefore, you do not need to read the whole guide, but you can go straight to the function that you need. As IMI develops further, more modules may be added to it and extra chapters added to this guide.

The chapter on 'the role of coordinators' is mainly addressed to **IMI coordinators**, but even if you are not a coordinator, it may help give you a general understanding of a coordinator's tasks. The final chapter gives an overview of how **personal data** is protected in IMI.

This guide focuses on the **technical aspects** of using IMI. It does not provide guidance on content issues such as the extent of your obligation to cooperate under the different pieces of legislation for which IMI is used, or in which precise scenarios to use it. There are a number of more specialised training documents available on the **IMI website** that provide this guidance (e.g. the User Guide to IMI and the Services Directive and the Guidelines for the alert mechanism in IMI). The IMI website can be found at:

❯ **http://ec.europa.eu/imi-net**

Most importantly, the IMI website contains **the link to the IMI system** and to the IMI training database, an identical copy of IMI without any real data in it. It also provides training materials on individual IMI functions, a **Frequently Asked Questions** document and an **IMI glossary**. Help on specific steps in the process of using IMI is available in the system through a series of **'info points'**, clickable icons that display additional information about specific fields.

If you need further assistance or if you would like to give feedback on IMI, please contact your **National IMI Coordinator (NIMIC)**, who is responsible for the overall deployment and smooth running of IMI in your country. Depending on the organisational structure of IMI in your country, the NIMIC may have set up a **national IMI helpdesk** or a number of decentralised support points. You can find their contact details on the IMI website and inside the IMI application.

The European Commission has also set up a **central IMI helpdesk**. If the NIMIC cannot resolve a problem locally, he or she can contact the Commission helpdesk at:

❯ **imi-helpdesk@ec.europa.eu** or by telephone at **0032-2-29 55470**.

2. The basics

This chapter gives an overview of how the IMI system works and who is involved. It describes some of the roles that competent authorities can have in IMI and the different user profiles.

2.1. What is the IMI system?

Various pieces of internal market legislation make it mandatory for competent authorities in the European Economic Area (EEA)[1] to assist their counterparts in other countries by providing them with information. Some legislation also stipulates communication between Member State authorities and the European Commission. IMI is an electronic tool designed to enable competent authorities to carry out this day-to-day exchange of information. It has been developed by the European Commission, in close cooperation with the Member States.

IMI is a single system used in different legislative areas, such as the recognition of professional qualifications (Directive 2005/36/EC) and the supervision of migrating service providers and cross-border provision of services (Directive 2006/123/EC). IMI is being expanded to cover additional areas.

2.2. How does IMI work?

IMI facilitates the exchange of information between competent authorities by enabling them to easily find their counterparts in other Member States and to communicate with them quickly and efficiently. It helps overcome practical barriers to communication, most importantly differences in administrative structures, languages and a lack of clearly identifiable partners in other Member States.

IMI is made up of individual building blocks (**modules**) that can be used independently. These are the main modules:

- A **directory of competent authorities** throughout the EEA who are involved in the day-to-day application of internal market legislation. The directory is equipped with multilingual search functions.

❯ Overcoming the language barrier — the 'art of the possible'

To facilitate communication between authorities across Europe, IMI works with **predefined and pre-translated questions and answers** available in all official EU languages. A user in an Italian authority can select a series of questions in Italian and send the request to Hungary. The Hungarian user will see the questions in Hungarian and select a pre-translated reply. The Italian authority will then receive the reply in Italian.

For more complex cases, authorities will need to provide further details in **free text**. To minimise the language barrier in such cases, IMI offers two levels of support:

– it indicates the languages understood by the users in each competent authority;

– it provides online machine translation for specific language pairs for a rough translation of free text.

As an IMI user, you should try whenever possible to use a language understood by the authority you are contacting. **Write as clearly as possible and use short sentences**. Remember that machine translation can only give a rough idea of the translated text; for legal purposes it may still be necessary to obtain an official translation, depending on the context.

[1] The EEA consists of all EU Member States as well as Iceland, Liechtenstein and Norway.

- A workflow for **exchanging information** between competent authorities. This uses lists of pre-translated questions and answers (each based on a specific piece of legislation supported by IMI) available in all EU languages. It allows users to attach documents and to monitor and follow-up pending information requests.
- A workflow for sending, receiving and disseminating **alerts**, as required under the Services Directive.
- A **directory of registers** maintained by competent authorities throughout the EEA. This directory also has a multilingual search function.

2.3. Who is involved in IMI?

2.3.1. Competent authorities

The main actors in IMI are the **competent authorities** throughout the EEA who use the system to **exchange information**. These authorities may be public-sector bodies or private bodies delegated by the Member States to carry out certain functions related to the application of internal market legislation. They may operate at **national, regional or local level**.

2.3.2. IMI coordinators

IMI also involves a number of **IMI coordinators**, whose role is to authenticate competent authorities requiring access to the system, provide technical support and ensure that requests from other Member States receive satisfactory replies in a timely manner (= **administrative role**). Like competent authorities, coordinators can also exchange information with other authorities registered in IMI.

In addition, IMI coordinators may also play a coordinating role in relation to specific workflows in IMI. For instance, a Member State may decide that all requests need to be approved by an IMI coordinator prior to being sent to another Member State (= **content-related role**).

Each Member State has one National IMI Coordinator (**NIMIC**). At the discretion of the Member State, Delegated IMI Coordinators (**DIMIC**s) may be nominated to take over some or all coordination responsibilities for a particular legislative area, a division of the administration or a geographical region. In the special case where a regional DIMIC has responsibility for all legislative areas for its region, it is known as a Super-DIMIC or SDIMIC. An IMI coordinator who is responsible for overseeing a whole legislative area on behalf of a whole country or a federal region is called a **LIMIC**.

2.3.3. European Commission

The **European Commission** hosts and maintains the IMI system in its Data Centre in Luxembourg. It is responsible for the translations in the system and provides a central helpdesk to assist Member States in using IMI.

2.4. Authority roles in IMI

Regardless of its administrative role (whether IMI coordinator or competent authority), an authority registered in IMI may play one of several content-related roles in a workflow to which it has been given access. The following table gives an overview of these roles.

Administrative role	Content-related role	
Authority type / Legislative area role	**Workflow role**	
	Information request	**Alerts**
Coordinator role: NIMIC SDIMIC LIMIC DIMIC	Request Coordinator	Alert Coordinator Incoming Alert Postbox
Competent Authority	Authority (Requests)	Alert Authority

In addition to these roles, IMI coordinators may also have one or both of the following administrative roles: **validating coordinator**, i.e. the coordinator that registers and/or validates an authority in IMI, and **access coordinator**, i.e. the coordinator responsible for granting and managing an authority's access to a particular legislative area and workflow. Each authority has one validating coordinator and one access coordinator per legislative area.

For details on the different **administrative roles**, please see chapter 9.1.1. **Content-related roles are defined for each workflow** and you will find detailed descriptions of them in chapters 5 and 6.

It is important to note that an authority's content-related role does not depend on its administrative role. For instance, a Ministry of Public Administration can be the NIMIC, it can have the role of Authority in the requests workflow for Professional Qualifications and it can play the role of Incoming Alert Postbox in the alerts workflow for the Services Directive. Similarly, a National Chamber of Commerce and Industry can be a DIMIC for the Services Directive, the Request Coordinator in the information exchange (requests) workflow, and the Alert Authority in the alerts workflow.

2.5. User roles

Each registered authority/coordinator nominates one or more physical persons within the authority as IMI user(s). **Each user needs to be registered** in the system and is granted a defined set of **user rights** that control what he or she can do in the system.

Authorities registered in IMI vary considerably in size and organisation. To accommodate that, the system offers a flexible set-up. At one end of the scale, a small authority dealing with a low number of requests may choose to authorise just one or two users to carry out all activities in the system (**it is recommended to register at least two users** to ensure back-up during holidays or sick leave). At the other end of the scale, a large authority (for example a Medical Chamber) may have a big department dealing with the recognition of professional qualifications and may need to manage a high number of information requests. In this case, it would need to register several IMI users with clearly defined areas of responsibility.

Each registered IMI user may belong to only **one** competent authority or coordinator.

The following table provides an overview of all user roles available in IMI. Some are general, as they are not related to a particular workflow. Others are specific to a module from an IMI legislative area.

General	Information requests	Alerts
Local data administrator Data administrator *(only for coordinators, per legislative area)* Basic user	Request viewer Request handler Allocator Referral handler *(only for coordinators)*	Alert viewer Alert handler Alert disseminator *(only for coordinators)*

The general user roles are explained in chapter 4 (local data administrator and basic user) and chapter 9.1 (data administrator). User roles specific to the information request workflow are explained in chapter 5.2.2. For user roles relating to the alerts workflow, see chapter 6.2.3.

3. Accessing IMI

This chapter explains how registration in IMI works, in particular if you register in response to an invitation from an IMI coordinator (= self-registration).

It also explains the procedure for logging in to IMI, which is the same for all IMI users.

IMI is a secure online application available only to **registered competent authorities**. IMI coordinators are responsible for identifying the authorities that should use IMI and for their registration in the system. A coordinator may decide to register a new competent authority or invite the authority to register itself in IMI.

3.1. Registration in IMI

Registration in IMI follows a number of steps in which information about the new authority needs to be provided. These steps are very similar whether the registration is carried out by a coordinator or whether the authority is registering itself. For self-registration, a few additional steps need to be taken, as described below.

3.1.1. Registration by an IMI coordinator

In most cases, an IMI coordinator will register your authority in IMI. Prior to this, you will probably have been in touch with your coordinator and will have had to provide them with certain data such as basic information about your authority and the person who will be registered as the first user in the authority.

Once the coordinator completes your authority's registration, he or she will contact you to give you your username. You should then log in to the system and check that the data recorded in IMI about your authority is correct.

> **If you are the first user of your authority, please read the sections on local data administration (chapter 4).**

> **If you are an IMI coordinator, please read chapter 9 for specific guidelines for coordinators on self-registration, registration of authorities and registration of IMI coordinators.**

3.1.2. Self-registration: guidelines for competent authorities

Depending on your authority's areas of competence, an IMI coordinator may decide to invite you to register in IMI for one or several of the legislative areas and workflows that it coordinates.

3.1.2.1. Invitation to register in IMI

You will receive an **email** informing you that your authority is invited to register in IMI. In this email you will find the name of the IMI coordinator who sent you the invitation and their email address.

The invitation email will also include a **link** to the IMI registration page and a unique **registration code**, needed to start the registration process. Please note that the registration code is only valid for **30 days**. If you have not registered five days before your registration code expires, you will be sent a reminder.

3.1.2.2. Self-registration: step-by-step

> **Security checks**

When starting the registration process, you must pass a security check requiring you to type a randomly generated code displayed on the screen (captcha code). You will also have to enter the registration code received by email.

The security check may fail for one of the following reasons: the registration code is not valid (e.g. has expired), the invitation to register has been withdrawn by the coordinator or another user in your authority has already used the code to register. If your registration code is not accepted, please contact the coordinator who invited you. They may need to reissue your invitation.

> Entering authority data

Once you have successfully passed the security check, the system will guide you through a series of screens asking you to enter information about your authority. This includes the authority name, its contact details and information about your authority's areas of competence. You can find more details about authority data in chapter 4.

> First user details

When registering your authority in IMI, you will also register a first user, who will be able to log in to the system once your registration has been validated. Please make sure that you enter a **valid email address** for the user, as they will receive important notifications by email following this registration.

The first user will receive by default 'local administrator' rights, as well as any roles specific to the workflow(s) for which his or her authority has been invited to register.

> Legislative area settings

IMI is designed to support many pieces of Internal Market legislation. When inviting you to register in IMI, your coordinator will indicate which legislative area(s) you should have access to. During the self-registration process, you must provide certain details about your authority's competence in each of these areas. More precisely, for each legislative area concerned, you have to select from a list of **keywords** those that best describe your authority's competence. Please note that by default the system will assign you the role of 'Competent Authority' at the legislative area level. Before validating your registration, your validating coordinator may, however, decide to give your authority a different role.

> Completing the self-registration

Before completing the registration, the system will display a **summary** of the data entered in each of the previous steps. This summary will also include a system-generated **username** for the first user registered for your authority. Once the registration is validated by your coordinator, the first user will need this username to log in to the system.

To ensure that you keep a record of this username and the data entered during the self-registration, the system will ask you to **print** the registration summary or to **save** it as a Word document on your computer. You will only be able to exit the registration process after printing or saving the summary.

3.1.2.3. Registration completed: what happens next?

After registering, you will receive an email confirming that your authority's data has been successfully **recorded in IMI**. This message will include a **summary** of the information you entered (except for the username).

At the same time, your coordinator will be notified that you have completed the registration process and that she or he needs to **validate** the newly registered authority.

Upon validation by your coordinator, you will receive a new email informing you that your authority has been granted **access to IMI**. This email will include a detailed explanation of the procedure for logging in to the system and a link to the e-learning material available on the IMI website.

3.2. Logging in to IMI

In order to access the IMI system, you must be a **registered user** with three separate pieces of information: a username, password and security code.

3.2.1. Username and temporary password

As soon as you are registered as an IMI user, you will receive your **username** from the local data administrator of your authority. If you are the first user of your authority, you will receive your username from the IMI coordinator who registered your authority. You will receive your username outside the system (e.g. by telephone or in person).

If you register your authority yourself in response to an invitation from an IMI coordinator, your username will be provided to you at the end of the self-registration process (see also chapter 3.1.2.2).

Once you are registered as a user, you will receive two emails automatically generated by the IMI system. The first email contains **instructions** explaining how to log in to the system. The second email (sent within 48 hours after registration) will contain your **temporary password**. If you are the first user of your authority, this email will also contain an explanation of which data and settings you should update when you log in to IMI for the first time.

3.2.2. First login to IMI

To log in for the first time, enter your username and temporary password. You will immediately be asked to change the temporary password to one of your choice. Please keep a safe record of your new password.

When you have changed your password, the system will ask you to create and confirm a 12-character **security code**. This code should be a combination of letters, digits and symbols. Please keep a safe record of this code.

3.2.3. Subsequent logins

Once you have your username, password and security code, you can log in to the IMI system at any time. Each time you want to log in, you will be asked to enter your username, password and three randomly selected characters from your security code. Please note that IMI is case-sensitive.

3.2.4. Incorrect username, password or security code

You are given five attempts to log in. If you do not enter the correct username/password/security code combination during these five attempts, your user account is blocked and your password must be reset.

> **You have forgotten your username:**

If you cannot remember your username, please contact a local data administrator in your authority. He or she will send you a username outside the system.

If you are the only local data administrator in your authority or if, for any reason, you cannot get in touch with your local data administrator and you have forgotten your username, please contact your IMI coordinator (the coordinator responsible for your authority's access to IMI) who will be able to assist you.

> **You have forgotten your password or security code:**

If you have forgotten your password or security code, please contact a local data administrator of your own authority. He or she will reset your password. You will then receive an automatic email with your new temporary password. You can now log in again as described under point 3.2.2.

If you have forgotten your password or security code and are the only local data administrator in your authority, please contact your IMI coordinator. He or she will reset your password. You will then receive an automatic email with your new temporary password. You can now log in as described under point 3.2.2.

4. Managing your authority in IMI

This chapter explains the role of local data administrator and how to update the information about your authority and its users in IMI. It also explains what information is held in IMI about each authority and how this should be kept up-to-date.

Once registered in the IMI system, **each authority is responsible for its own local data management**. 'Local data administrators' are crucial to this task. Their role is one of the general user roles available in IMI.

❯ **User role: Local data administrator**

Users with local data administrator (LDA) rights can update data held in IMI about their authority and can register additional users in their authority. They can change the user rights and reset passwords for all users in their authority.

By default, the first user of a competent authority receives the role of local data administrator. The default setting can be changed and the role assigned to another user. It is also possible to have two or more LDAs by assigning the role to further users.

4.1. Authority data and competencies

4.1.1. General information about your authority

It is important to keep the information about your authority in the IMI system as up-to-date as possible. This will help IMI users in other Member States to identify the correct authority to contact. It will also ensure that automatic emails sent by the IMI system are sent to the correct email address.

The general information on your authority includes:

> **Authority name and informal title**

Providing the **official name** of your authority is part of your registration in IMI. After registration, you will not be able to edit your authority's official name. If it is incorrect, please advise the IMI coordinator responsible for your authority's registration. He or she can edit the name.

In addition, IMI allows each authority to choose its own **informal title**, a version of its name that clearly states what the authority does. This informal title is translated into all EU languages. In order to help others identify an authority in the system, the informal title should be short and clear.

> **Authority description**

On its own, the informal title is unlikely to be enough to fully convey what your authority does. You may write a **short profile** of your authority in your official language and IMI will provide the online translation. Here you can indicate, for example, whether your authority is local, regional or national, its main fields of activity and its tasks in these fields. The short profile should cover only aspects that are relevant for the purposes of your authority's role in IMI.

> **Languages**

IMI allows you to identify all the **languages understood** within your authority. Although IMI provides pre-translated questions and answers, sometimes IMI users in other countries may want to add a question or a comment in free text. In such cases, it would be very useful for them to know which languages are understood in your authority.

> **Contact details**

You will also be asked to enter basic contact data about your authority, including **address, telephone number** and **website**. You must also provide **a contact email address** for the authority. Please ensure that this email account is checked regularly, as it will be used for important communications from the system to your authority.

4.1.2. Areas of competence

In order to assist other IMI users in finding the right authorities to contact in other Member States, each authority is asked to provide more detailed information about its areas of competence. Your area of competence can be defined by selecting entries from pre-defined lists of economic activity and policy areas.

The **areas of economic activity** are based on NACE, the 'Statistical Nomenclature of Economic Activities in the European Community'. This provides a hierarchical structure of all economic activity. The **policy areas** are based on a list of all policy areas of European relevance and are also listed in a hierarchical structure. For each list, you can choose one or more entries which describe your authority's competence.

You may not find a perfect fit for your authority's area(s) of competence in those lists. Please take a pragmatic approach and choose the best possible combination of economic activities and policy areas.

It is also possible to indicate that your authority has **general horizontal competence**, i.e. is competent for all economic and policy areas in a specific geographic area. In some Member States this is the case for municipalities, for example. In IMI, this setting is applied by default to all NIMICs and SDIMICs.

4.1.3. Legislative area and workflow settings

4.1.3.1. Legislative area descriptive data

You must also provide information about your authority's competence in each legislative area to which it has access.

To help you with this task, IMI provides you with **lists of keywords** for each legislative area. You must select at least one entry during your authority's registration in IMI. Local data administrators of your authority should check that the selection of keyword(s) is appropriate and update it if necessary.

NIMICs and SDIMICs are by default registered for all keywords, as they have general horizontal competence. This cannot be changed.

4.1.3.2. Workflow settings

For each legislative area to which it has access, a competent authority will also be granted access to one or more of the workflows that support it (for example, for services, to the information request workflow and the alert workflow). In addition, for each workflow, certain settings (= **flags**) can be activated to define the actions that the authority can take.

Most of these flags are defined by the validating coordinator upon registration or validation of the authority in IMI. Later on they can be changed by the access coordinator (the coordinator responsible for access to the legislative area in question). The workflow settings managed by IMI coordinators are explained in more detail in chapter 9.1.4.

For the information request workflow, each authority can activate the **allocation flag**, which allows you to distribute incoming and outgoing requests to relevant users in the same authority. You can read more about allocation in chapter 5.3.5.

4.1.3.3. Linked coordinators

Each competent authority is linked to one or more content-related coordinators for each workflow to which it has access. For the request workflow, a **linked coordinator** will be able to view the details of the authority's information exchanges, excluding any personal data. Linked coordinators may also play a role in the **referral process** or in the **approval process** (see chapters 5.3.6 and 5.3.7). In the alert workflow, a coordinator linked to an alert authority may play the role of alert coordinator (see chapter 6.2 for more details).

A competent authority may be linked to more than one coordinator in a legislative area. For example, in the Services module, a regional board of architects could be linked both to the national board of architects and to the ministry of economy. Depending on the content of each request, the regional authority can decide to link either of the two coordinators to that request.

Linked coordinators are defined by the validating coordinator upon the authority's registration or validation in IMI. These relationships can also be updated later on by the authority's access coordinator for a specific legislative area. In addition, the local data administrator of the authority may add or change its linked coordinators as appropriate.

4.2. User management

Each registered authority has to nominate at least one person as an IMI user. The first user in each authority receives all the user rights available for the IMI modules to which the authority is granted access. Every additional user registered for the authority will be at least a **basic user**. Further rights can be granted to basic users in order to give them access to additional IMI functions. Basic users can search for a competent authority registered in IMI and can consult the directory of registers held in IMI.

Any user with local data administrator rights can then **register additional users** as necessary. Each user will be granted a defined set of user rights that dictate what he or she can see and do within IMI.

To register a new user, you must enter the following information:

> name and surname

> preferred working language (in which the user will receive all email communications from IMI)

> email address — this email address will be used for all system-generated automatic emails that involve this user. Each new registered user must have a different and individual email address.

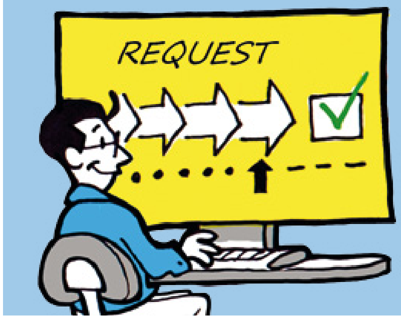
> telephone number (optional)

> user rights — you define which rights the new user will have for each legislative area and workflow.

It is possible to change the user rights at any point in time. If you are a local data administrator in your authority, you will be responsible for managing user rights for all users of your authority. Note that, depending on the authority's role in IMI, certain user roles must be attributed to at least one user in the authority.

User roles specific to the information request workflow are explained in chapter 5. For user roles relating to the alert workflow (Articles 29 and 32 of the Services Directive), see chapter 6 of this manual.

5. Handling requests



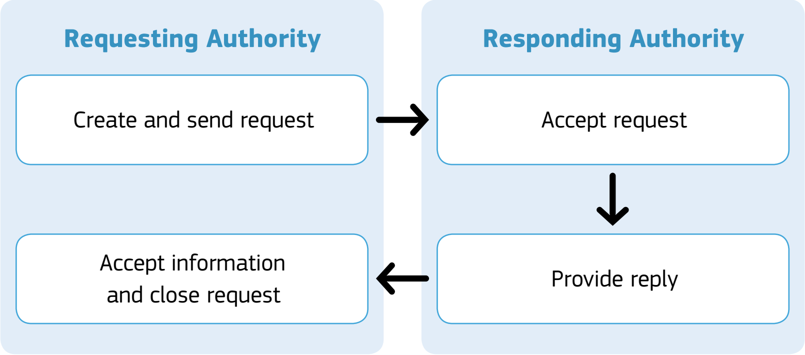
This chapter explains how to handle an information request in IMI. It outlines the main steps in the process, from the basic request lifecycle to more complex procedures. It also describes the actors involved in a request, their roles and the settings that determine what each actor can do. You will learn how to track your requests and find out about the report facility and the role of coordinators in the process.

A key function of IMI is to support information exchanges between authorities in different Member States in the EEA. The IMI module that allows for one-to-one communication between competent authorities is known as the **request workflow**. An individual query sent through the system is known as an **information request** or simply a **request**.

5.1. The request lifecycle

There are four steps in the lifecycle of a request:

1. A competent authority registered in IMI for the request workflow can **create and send a request** for information to a counterpart in another Member State. The content of the request depends on the legislative area and on the specific situation. The authority that sends the request is known as the **requesting authority**.
2. The competent authority that receives the request for information checks the details of the request such as the questions asked and certain data about the subject matter (no personal data is displayed before taking responsibility for a request). The **responding authority** decides whether it is competent to deal with the request and if so, **accepts** it.
3. The responding authority provides answers to all the questions contained in the request and **sends the reply** to the requesting authority.
4. The requesting authority checks the answers received and if satisfied with the reply, **closes the request**.


Requesting Authority

Responding Authority

Create and send request

Accept request

Provide reply

Accept information and close request

The request lifecycle may include additional steps, for example, when the requesting authority is not satisfied with a reply and asks for additional information. If the responding authority maintains that it cannot provide the requested additional information, the request may be referred to an IMI coordinator to seek its opinion. In this chapter you can find more details about the **alternative flows** of an information request.

5.2. Request actors and their roles

5.2.1. Authority roles for requests

When authorities are granted access to the request workflow, they are assigned a role either as an **authority (requests)** or **request coordinator**. These roles are defined for each legislative area and are independent from other roles that the authority concerned may play in IMI in other respects.

5.2.1.1. Authority (requests)

A competent authority with the role "authority (requests)" can send and receive requests for information relating to a particular legislative area. It must be linked to at least one request coordinator. If an authority is linked to more than one request coordinator, it needs to select the right one for each request.

5.2.1.2. Request coordinator

A request coordinator can be linked to a competent authority with access to the request workflow. The request coordinator may intervene if there are problems in handling a request involving an authority that it coordinates. The coordinator's intervention depends on its workflow settings (or flags), as explained in chapters 5.3.6 and 5.3.7. In addition, request coordinators can send and receive requests.

5.2.2. User roles for requests

5.2.2.1. Request handler

A user with request handler rights can send and answer information requests on behalf of his authority. He can also search for a competent authority registered in IMI and can view high level information about requests of other authorities in his country. This user profile is available in any authority with access to the request workflow, including authorities with the role of request coordinator. There must be at least one request handler in each authority with access to the request workflow.

5.2.2.2. Request viewer

Request viewers can view, save or print the full details of requests to which their authority has access (including personal data contained in them), without being able to take any action.

5.2.2.3. Allocator

Some larger competent authorities with a high number of users may wish to allocate incoming requests to a subset of the authority's request handlers, depending on the subject matter or other criteria. For example, a large authority that registers professionals may have different teams responsible for applications from different countries. The allocation process makes it possible to assign any new IMI request received by the authority to the correct team.

The allocator can assign requests. When the authority activates the allocation process, there must be at least one allocator in the authority. The local data administrator(s) in the authority automatically receive allocator rights. They may decide to give this profile to other user(s).

5.2.2.4. Referral handler

A referral handler is a user within a request coordinator who is involved in the referral process. Referrals are a way of escalating a disagreement between competent authorities over an information exchange to their coordinators. The request coordinators decide whether or not to participate in referrals. If they participate, it is up to the referral handler to examine the request and the response and to give his opinion as to whether he considers the response satisfactory. Referral handlers can view the details of requests involving coordinated authorities, except for any personal data. There must be at least one referral handler in each authority with the role of request coordinator.

5.3. Handling requests in IMI

5.3.1. Creating and sending requests

To create and send an information request in IMI, you need to have **request handler** rights for the legislative area concerned.

If your authority has access to more than one legislative area in which the requests module is used, you will have to select the correct legislative area for each request.

❯

Search for a competent authority

An important step in the request creation is identifying the authority that you need to contact. Different **search criteria** are available to help you. For example, you can use lists of keywords specific to each area covered by IMI. These are the same as the ones selected for each authority during registration.

IMI also allows you to search by entering your own keywords. The free text search returns only exact matches and is sensitive to special characters. For example, if you are searching for a French *'préfecture'*, you will not find it if you type 'prefecture'. You will find more details on how the free text search works by clicking on the 'info point' available in the system.

If you cannot find the competent authority to which you think your request should be addressed, you should send your request to an IMI coordinator in the receiving Member State who is responsible for the legislative area or the region that you are interested in.

For each request, you will have to provide details about the case, some of which will be mandatory.

You may also have to provide a **justification** for sending the request and set an **indicative deadline**. Before accepting your request, the responding authority may accept this deadline or propose a different one.

IMI provides pre-defined questions grouped in broad categories (= **question sets**). If there is more than one question set for a legislative area, you need to choose the one containing the questions you wish to send to your counterpart. Only one question set may be chosen per request.

You must select **at least one question** from the selected question set. If necessary, you can add comments to the question in free text.

❯

Free text comments

IMI allows you to enter comments after each pre-defined question. For each free text comment, you need to specify the language in which you have entered your text. This will allow the other authority to use the machine translation service to obtain a rough translation of your comment.

On the screen, you will also find out which languages are spoken by the other authority. Where possible, it is advisable to enter your free text comments in one of those languages. This will facilitate communication and reduce the need to use machine translation.

You will also be able to **attach one or more documents** and ask questions related to your attachment(s).

As you enter the required data for the new request, you will be able at any point to **save the request as a draft** and work on it again later. You can find your draft requests in your action list for requests.

5.3.2. Dealing with incoming requests

When your authority receives a request, you will be informed by email. This email will be sent to all users with request handler rights or, if your authority uses allocation (see chapter 5.3.5.), to all users with allocator rights. In addition, an email will be sent to the contact email address of the authority.

5.3.2.1. Accepting a request

As a request handler, you can accept new requests sent to your authority. You will see the new requests in your action list for requests with the status 'Awaiting acceptance'.

When you first open a new request, you will see a summary of the important details of the request, **except for any personal data** that would allow you to identify the request subject (for example the professional). Until you accept responsibility for the request on behalf of your authority, you are not confirmed as the responding authority and therefore should not be able to identify the request subject. As personal data may be included in documents attached to the request (e.g. certificates or diplomas), you will **not be able to open the attached file(s)** until you accept a request.

You will, however, be able to **see all questions and comments in the request, including those related to attachments**, before accepting a request.

Should you consider the deadline indicated by the requesting authority to be unfeasible, you may **propose a new date** for replying to the request.

If your authority is linked to more than one request coordinator, you will have to **select the appropriate coordinator** when accepting a new incoming request. For example, if your authority has competences both for tourism and catering services, and if the request relates to catering, you should select the coordinator for the catering sector. You will be able to change the request coordinator, if necessary, at a later stage in the request lifecycle.

❯ **Refusing a request**

In exceptional circumstances, a competent authority may decide to **refuse** a request outright. The option to refuse a request will only be available to competent authorities that have been authorised by their IMI coordinator to do so. IMI coordinators also have the option to refuse a request on behalf of their Member State. Refusing a request implies that the request will be closed straight away. You should only refuse a request if you are certain that there is no other authority in your Member State competent to deal with the request. If you do refuse a request, you will be asked to provide a justification for doing so.

5.3.2.2. Replying to a request

Once you accept a request, you will be able to view all the details and the documents attached to it. For each question, you will be able to select from a list of **pre-defined answers** or to enter **your own comments** to reply.

Please note that IMI allows the two authorities involved in a request to communicate with each other **before a reply is provided**. For example, the responding authority may ask for further details or further supporting documents about the case or may wish to provide some information in advance, before actually replying to the request. In turn, the requesting authority may wish to add further details or clarify points raised by its counterpart. This communication is carried out using the **structured messages** that can be added to the request. Once a new message is saved by one of the authorities, the other one will be informed by email that new details have been added to the request.

The two competent authorities can also **attach further documents** to the request during the process. Specific pre-defined comments will allow them to explain their relevance for the case.

5.3.2.3. Forwarding a request

As you check the details of the incoming request, you may find your authority is not competent to deal with that request. In this case, you can **forward** the request to another competent authority or IMI coordinator in your Member State. You will be asked to provide a justification for doing so. Once you have forwarded a request, you no longer have any responsibility for it. The requesting authority will be informed by email that a new responding authority is now expected to deal with the request.

It is also possible to forward the request after having accepted it. **If you forward an accepted request, any draft answers or comments that you have entered will be lost**.

5.3.2.4. Splitting a request

In some cases, you may find that your authority is only partially responsible for the content of the incoming request. For example, you will be able to answer one question included in the request, but you do not have the competence to deal with the other questions. In this case, you can **split the request** by forwarding one or more questions to another authority or an IMI coordinator in your Member State. You can also forward one or more documents attached to the original request, but a copy of the forwarded document will also remain in the original request. You will be asked to provide a justification for splitting the request.

Once you split the request, you will no longer have any responsibility for the forwarded questions and will only have to reply to the remaining ones. You will still have access to all the attachments included in the original request. The questions and attachments you forward will become a new separate request.

The requesting authority will be informed by email that its request has been split and a new responding authority is now expected to deal with some of the questions in its request.

5.3.3. Closing requests

As a request handler who deals with a request sent by your authority, you will be informed by email that a reply has been provided to the request. A copy of this email will be sent to the contact email address of your authority. You will also find the request in your action list for requests.

You can then **check the answers** to the questions contained in your request and read any free text **comments** added by the responding authority. The reply may also contain **attachments** you can view.

If you had included an attachment in your request and asked questions related to it, remember to check the responses (and any comments) provided.

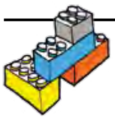
Once you have assessed the reply to your request and are happy with it, you must acknowledge it as satisfactory. If you accept the response, the request will then be closed. Closing the request is important, as after a certain time from closure, any personal data contained in the request will be removed from the system. For more details on data protection in IMI, see chapter 10.

If you close a request but then find out you need further information about the same case, you can use the copy request option explained in chapter 5.3.8.

5.3.4. Asking for and providing additional information

5.3.4.1. Asking for additional information (Requesting authority)

As a request handler in a requesting authority, you may find that a reply you have received is not satisfactory. If so, you can **request additional information** from the responding authority. You will have to provide a justification for doing so.



You should only ask for additional information in relation to the original questions included in your request. If you wish to ask new questions about the same subject, you should first close the original request and then use the 'copy request' function to create a new request.

If the responding authority **agrees to provide further information**, you will receive a new reply which you may consider sufficient. You can then close the request.

If the responding authority **refuses to provide further details**, several scenarios are possible. You may, for example, understand why the additional information is not available and decide to **close the request**. You may maintain that you need more information, in which case you should **refer the request** to a request coordinator to seek his or her opinion. This scenario is described in more detail in chapter 5.3.6.

5.3.4.2. Dealing with a request for additional information (Responding authority)

If a requesting authority is not satisfied with the response you provided to its request, it may send you a request for additional information. The system will notify by email the request handler in your authority who took the last action in relation to the request. A copy of this email will be sent to the contact email address of your authority. The request handler will also see the request in his or her action list.

> Accepting a request for additional information

If you feel you can provide the requested details, you should **accept** the request for further information. The request will remain in your action list until you send the additional information. After this, the requesting authority may consider your new reply satisfactory and close the request.

> Rejecting a request for additional information

If you cannot provide the missing information, you can **reject** the request for further information. You will be asked to provide a justification for doing so.

The requesting authority will assess your justification and may accept that the information is not available. It will then **close the request**. If, however, the requesting authority finds your justification insufficient, it may decide to **refer the request** to an IMI coordinator for his or her opinion (see more details about the referral procedure in chapter 5.3.6).

5.3.5. Using allocation

The **allocation procedure** allows large competent authorities with a high number of IMI users or with mixed competence (with different users in charge of different areas) to assign information requests to one or more of its request handlers, depending on the subject matter or other criteria. The allocation setting can be activated and deactivated by the authority's local data administrator(s).

In order to be able to assign and re-assign requests within the authority, a user needs to have **allocator** rights.

A request can be allocated at any time throughout the request lifecycle.

5.3.5.1. Allocation of incoming requests

When an authority receives a new incoming request, the allocator(s) is (are) informed by email. They also see new requests in their action list. Allocators can open the request, view it (without personal details of the data subject) and assign it to one or more request handlers in the authority.

Whenever a request is assigned to a request handler or re-assigned to a different request handler, an automatic email is sent to the new request handler to inform him that a request has been allocated to him.

Only assigned request handlers can take an action on the request. All other request handlers have full access to the details of the request, but cannot take any action on it on behalf of their authority.

5.3.5.2. Allocation of outgoing requests

When a request handler creates a new request, he automatically becomes the assigned request handler for that request. The authority's allocator may assign the request to additional request handlers once it is saved as a draft. Otherwise the request handler who created the request will remain the only assigned request handler and only he will be able to take action on the request.

5.3.5.3. Use of allocation within an IMI coordinator

IMI coordinators may also decide to use allocation to assign any request in which they are involved as a requesting or responding authority. When they play the role of request coordinator, they will also need to allocate requests requiring approval or which have been referred to them for their opinion.

Only users with **referral handler rights** can be assigned a request needing the approval or intervention of their authority as request coordinator. The assigned referral handler(s) will then be able to take the relevant action (approve or reject the sending of a request/response and agree or not that additional information is not available). All other referral handlers also have access to the requests but will not be able to take any action.

5.3.6. The referral procedure

If the requesting authority maintains that it must receive additional information, it may decide to involve its coordinator (= **requesting coordinator**) and the responding authority's coordinator (= **responding coordinator**) as referees. This procedure is called **referral**.

Request coordinators decide whether they wish to be involved in referrals. Depending on their settings, the following scenarios are possible:

1. Only the requesting coordinator accepts referrals

The requesting coordinator will be asked by the requesting authority to give its opinion as to whether the response provided is satisfactory.

If it agrees that the response is not satisfactory, it will send the request back to the responding authority. The latter may reconsider its previous decision and accept to provide further information. Or it may uphold its previous position on the case and close the request.

If the requesting coordinator disagrees with the requesting authority's view and considers that the response is satisfactory, it may close the request.

2. Only the responding coordinator accepts referrals

In this case, the request referred by the requesting authority will go directly to the responding coordinator to seek its opinion.

If the responding coordinator agrees that the response is unsatisfactory, it will return the request to the responding authority. The latter may reconsider its previous decision and accept to provide further information. Or it may maintain its initial position, in which case the referral process starts again.

If the responding coordinator disagrees with the requesting authority's view and considers that the response is satisfactory, it may close the request.

3. Both coordinators accept referrals

First, the requesting authority refers the request to the requesting coordinator. If it agrees that the response is not satisfactory, the request will be referred to the responding coordinator. The involvement of two coordinators is described in points (1) and (2) above.

4. Neither of the coordinators accepts referrals

In this case, the two competent authorities need to resolve the case without their coordinators' intervention. After the responding authority has refused to provide additional information, the requesting authority may ask for it once again. The responding authority may decide to reconsider its previous decision and agree to provide further information. Or it may maintain its initial position and close the request.

5.3.7. The approval procedure

Some Member States have decided that IMI coordinators should retain a certain level of control over requests sent and received by the authorities they coordinate. This may be required by national administrative procedures.

In such cases, each coordinator needs to determine whether it will use the approval procedure for requests and/or replies of coordinated authorities and for which of these authorities it will do so. Chapter 9.1.4 explains how to manage the settings for the approval procedure.

If an authority is **subject to approval** and its request coordinator needs to **approve requests**, new requests created by the authority will not be sent directly to the responding authority, but will first be sent to the coordinator for review and approval.

Similarly, if an authority is subject to approval and its request coordinator needs to **approve replies**, any reply that the authority intends to provide will not go directly to its counterpart, but will first go to its coordinator for review and approval.

If a coordinator decides not to approve a new request/reply, it will be returned to the competent authority to be changed as suggested by its coordinator. The updated request/reply will then be sent back to the coordinator for review and approval.

5.3.8. Copying requests

The IMI system allows users to **create new requests from previous ones**. This can be useful, for example, when you need to send a request to an authority you have contacted before about the same subject or when you needs to ask the same questions as before. You can also ask new questions on an old subject if you need further information on a case you have already closed in IMI.

To use this function, you need to **open the request** that you want to use as the basis for a new one. Then select the data to copy over to the new request, e.g. the authority to contact, the questions or the attachments. Once the new request is created, you can add the remaining details.

A competent authority can copy any request it has sent or received, in any status of the request.

5.3.9. Keeping track of requests

IMI allows you to easily keep track of the requests sent and received by your authority using the dedicated action list and automatic email function.

5.3.9.1. Action list for requests

The **action list for requests** contains requests requiring you, as a user, to **take an action**. It is available to request handlers in competent authorities and to request handlers/referral handlers in IMI coordinators. If your authority uses allocation, a new incoming request or a request that is referred to you for the first time will initially be included in the action list of the user(s) with allocator rights. Once the allocator has assigned the request to one or more user(s) with request handler or referral handler rights, the request will appear on their action lists.

Depending on the status of the request, there will be different actions that you need to take on a pending request: accept and reply to it, consult a reply, close a request and so on. As a coordinator, you may need to approve a new request, reply before it is sent or intervene as part of the referral procedure. The action list for requests also includes draft requests of your authority.

Please check your action list for requests regularly. This will ensure that you handle your information exchanges in a timely manner and fulfil your obligations to cooperate with your EU counterparts.

5.3.9.2. Search for requests

Each authority has access at any time to all its incoming and outgoing requests, including draft, ongoing and closed requests. IMI allows users to identify requests based on different search criteria such as the request status, date when the request was sent or received or country to/from which a request was sent/received. Request co-ordinators can also search for requests for which they are linked coordinators.

5.3.9.3. Automatic emails

The IMI system has an automatic email function which informs users involved in an information request when they need to take action or when there is a significant development concerning the request.

The automatic emails briefly inform the user of the action to take and provide a link to access IMI. The emails never include details of the request itself.

When there is a **new incoming request**, there are two possible scenarios:

> **The authority does not use allocation:** an automatic email is sent to all users with request handler rights, copied to the authority's contact email address.

> **The authority uses allocation:** an automatic email is sent to the authority's user(s) with allocator rights. The authority's contact email address is put in copy. Once the allocator assigns the request to one or more request handler(s), the assigned request handler(s) will receive an automatic email informing them that a new request is awaiting acceptance.

Any subsequent email notifications related to a request are sent to the request handler **who has taken the last action**. A copy is sent to the authority's contact email address.

For **outgoing requests**, the requesting authority is informed, for example, when its request is fully or partially forwarded to another responding authority or when the reply has been provided.

As the two authorities involved can communicate via the comment fields, the request handlers will be informed by email every time a new comment is made by the other authority.

If a request is **referred to an IMI request coordinator for the first time**, there are two possible scenarios:

> **The coordinator does not use allocation:** an automatic email is sent to the coordinator's contact email address. Should the referral handlers within a coordinator not have access to this email address, the person responsible for managing the mailbox needs to inform the referral handlers that a new request has been referred to them (by forwarding the email or in any other way) and can be accessed through the referral handler's action list for requests.

> **The coordinator uses allocation:** an automatic email is sent to the coordinator's user with allocator rights. The coordinator's contact email address is put in copy. Once the allocator assigns the request to one or more referral handler(s), they receive an automatic email informing them that a new request has been referred to them.

For any subsequent automatic email related to a referred request, the automatic email is sent to the referral handler who has taken the last action. A copy is sent to the coordinator's contact email address.

5.3.10. Report facility

Competent authorities may wish to keep a record of requests received and sent through IMI. To this end, IMI enables users to generate, electronically save and print reports about IMI requests. The report facility is available at all stages of the request lifecycle, including when the request is in 'draft' status or after its closure.

Different types of reports can be generated, for example:

> **Full Report with Personal Data:** this includes all data recorded in IMI as part of a request: details about the requesting and responding authority, details about the data subject (including personal data), questions asked and answers provided, free text comments or questions and comments related to attached document(s).

> **Full Report without Personal Data:** this is similar to the previous report, except it does not include the personal data recorded about the data subject.

> **Customisable Report:** you may want to create a report containing only certain parts of the request. The system gives you a list of options, such as data about requesting/responding authority, details about the data subject, the questions asked, and so on. The report will include only the items you have selected.

> **Report for the Data Subject:** this can be generated at the request of the data subject, who may ask to see what information has been exchanged via IMI in relation to him or her.

- **Data Subject Consent Form:** in addition to the data included in the report for the data subject, this report includes a disclaimer and a consent form that the data subject can sign in order to agree to the exchange of his personal data.

Any user with access to the request workflow can generate reports related to the requests of his authority. If you only have allocator or viewer rights, you will only be able to generate reports without personal data.

Request coordinators can also generate reports concerning the requests of competent authorities to which they are linked. These reports never include any personal data. Reports are available for 30 days in a dedicated section in your activity panel.

Certified reports in IMI

IMI users have the option to ask for certified reports concerning their IMI requests. This is done by applying a corporate server-side electronic signature. The electronic signature applied on IMI reports is based on a qualified digital certificate issued by the Belgian Certipost to the legal representative of Directorate General for Internal Market and Services of the European Commission.

The electronic signature on IMI reports is based on the PAdES standard (PDF Advanced Electronic Signature). It assures the authenticity, integrity and non-repudiation of information request reports generated by the IMI system.

6. Handling alerts

(Art. 29 and 32 of the Services Directive)

This chapter deals with the technical aspects of handling alerts in IMI. It identifies the different roles that authorities and individual users can have in relation to the alert mechanism and it describes how to use all the functions available in IMI for each stage of the alert process. It also explains how to set up the system to deal with alerts effectively.

On the IMI website you will find further guidance on the conditions for sending alerts and possible scenarios.

6.1. The alert lifecycle

There are five steps in the basic lifecycle of an alert.

1. Any authority registered for the alert workflow in any Member State of the EEA can **initiate** an alert when it becomes aware of a dangerous service activity in its field of competence. It **submits** the alert to an alert co-ordinator in its own Member State. The alert coordinator **checks** the alert and **broadcasts** it to other Member States.
2. In each recipient Member State, the alert coordinator designated as the 'incoming alert postbox' **acknowledges receipt** of the alert. It **disseminates** it to the appropriate alert coordinators and alert authorities in its country. Alert coordinators can also **add further recipients**.

Note that 'submitting' and 'disseminating', in the context of the alert mechanism in IMI, always refers to actions taking place within one Member State. 'Broadcasting' means the sending of information from one Member State to other Member States.

3. The Member State of establishment (MSE) of the service provider concerned is responsible for **managing the closure** of the alert once the risk has been eliminated. If the MSE is not known, the Member State that initiated the alert is responsible for closure.

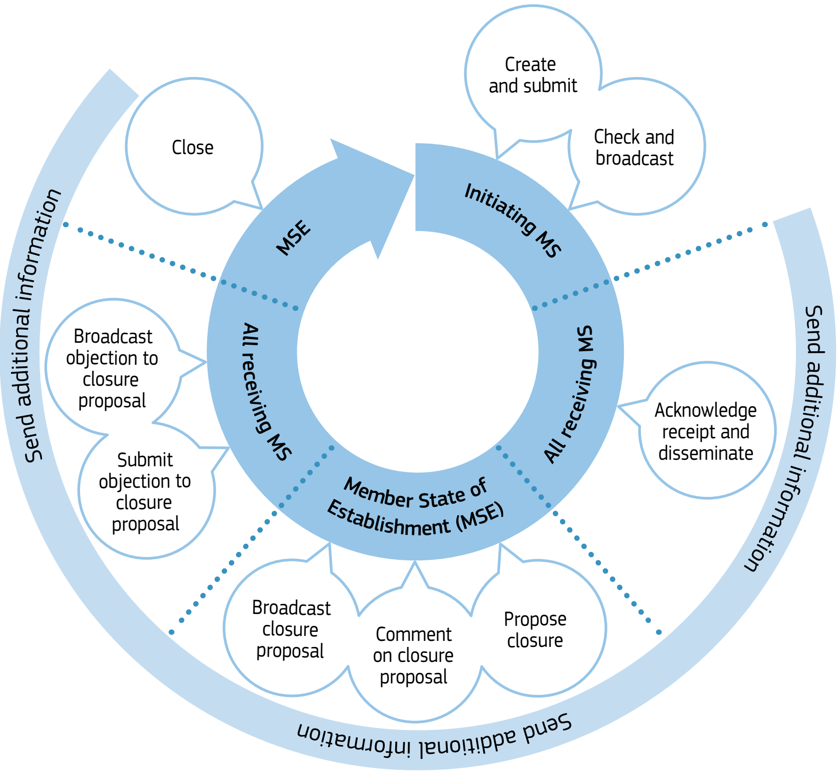
   Any authority that received the alert in the MSE can **initiate a proposal to close** the alert. All other authorities involved in the alert in that country can **comment on the closure proposal**. Once an agreement has been reached, a selected alert coordinator (the **'closing coordinator'**) can **broadcast the closure proposal** to all other Member States concerned.
4. Subsequently, all other Member States that received the alert have the option of **objecting to its closure** if they have information that the risk persists. Alert authorities **submit** objections as additional information to an alert coordinator, who can **broadcast** them to all other Member States involved.

Note that authorities in the Member State that proposes closure can 'comment' on a closure proposal before it is broadcast. Following broadcast, authorities in other Member States can 'object' to it.

5. Once it has been ascertained that the risk has been eliminated, the closing coordinator in the MSE can **close** the alert.

During the whole lifecycle of an alert and up to its closure, all Member States involved can add further information to the alert at any time.

Overview of the alert lifecycle


Create and submit
Check and broadcast
Initiating MS
All receiving MS
Acknowledge receipt and disseminate
Send additional information
Member State of Establishment (MSE)
Propose closure
Comment on closure proposal
Broadcast closure proposal
Send additional information
All receiving MS
Submit objection to closure proposal
Broadcast objection to closure proposal
Send additional information
MSE
Close

6.2. Alert actors and their roles

6.2.1. Authority roles for alerts

When authorities are granted access to the alert workflow in IMI, they are assigned a role either as **alert authority** or as **alert coordinator**. At least one alert coordinator will be designated as the **incoming alert postbox** for its Member State.[2] These roles are independent from the other roles that the authority concerned may have in IMI. For example, a national IMI coordinator (NIMIC) can act as an alert authority, and an authority that answers to a coordinator in relation to the standard information exchange can act as an alert coordinator.

6.2.1.1. Alert authority

Alert authorities are normally authorities with competences in the field of health and safety of persons or in the field of the environment. They can **initiate** an alert and **submit** it to an alert coordinator to which they are linked. They can also **receive** alerts that have been disseminated to them by the incoming alert postbox or by an alert coordinator and **react** to these alerts. They can **submit closure proposals** and **comment** on them. If another Member State proposes closure, they can **submit objections** to their alert coordinator.

6.2.1.2. Alert coordinator

The task of alert coordinators is to ensure that alerts are only broadcast when necessary and that they are handled properly. In general, they will have competences in the fields of health and safety of persons or the environment. They should also have a good overview of the administrative structures relevant to alerts in their Member State. Alert coordinators can **broadcast** alerts to other Member States and **add alert authorities and other alert coordinators as recipients** to incoming alerts. They can **broadcast additional information, including objections to closure**, and **broadcast proposals to close** an alert. Alert coordinators can also exercise all the functions of an alert authority. This means that, for example, they can initiate an alert and then broadcast it themselves.

6.2.1.3. Incoming alert postbox

An alert coordinator nominated as the incoming alert postbox is the central entry point for alerts in its Member

[2] In the interest of good coordination and for data protection reasons, the Commission recommends nominating a single incoming alert postbox per Member State. However, it is technically possible to register several postboxes, for example one for each region in a federal Member State.

State. It **acknowledges receipt** of an incoming alert and is responsible for the **initial dissemination** of the alert to alert coordinators and alert authorities in its Member State. It ensures that the alert is only forwarded to those actors (coordinators and/or authorities) that are competent to deal with it. This requires the incoming alert postbox to have good knowledge of the administrative structures of its Member State.

The incoming alert postbox also automatically **receives each alert sent out** from its Member State. This enables it to have an overview of all incoming and outgoing alerts.

The incoming alert postbox has all the action functions that alert coordinators and alert authorities have. This means, for example, that it can also initiate alerts and then broadcast them.

6.2.2. The 'final approval' setting for alert coordinators

IMI offers Member States some flexibility in defining the relationship between alert authorities and alert coordinators. Alert coordinators (including those flagged as incoming alert postbox) can be given the option to **edit or delete the content** of alerts or alert-related information before broadcast. If it is decided that an alert coordinator should have this option, a box in its **settings for the alert workflow** needs to be ticked, indicating that the alert coordinator has **'final approval'** for alerts it broadcasts on behalf of its Member State.

If a coordinator does not have final approval, the initiating authority retains the right to edit or delete the alert or alert-related information it submitted and which has not been broadcast.

6.2.3. User roles for alerts

When an authority is given access to the alert workflow within the IMI services module, the user in this authority who has the role of **local data administrator** (responsible for registering users and maintaining data concerning the authority) is automatically given all user rights for alerts.[3] He can then assign different user roles to his colleagues according to the size of the authority and their responsibilities for alerts.

6.2.3.1. Alert viewer

'Alert viewers' can **see the full details of all alerts** to which their authority has access (including personal data contained in them). They can save or print the full details of alerts, but **cannot take any action**, such as initiate an alert, update it or propose closure.

6.2.3.2. Alert handler

'Alert handlers' deal with alerts on behalf of their authority. They can **initiate** alerts and **submit** them for broadcast to an alert coordinator. They can **receive** alerts and **react** to them. They can also **submit additional information** relating to an alert. They can submit a closure proposal, comment on closure proposals submitted by other authorities in their own Member State and submit objections to closure if another Member State proposed closure. However, alert handlers in an alert coordinator **cannot broadcast or disseminate** alerts.

6.2.3.3. Alert disseminator (only for alert coordinators)

The user role 'alert disseminator' is only available to users under an alert coordinator. Alert disseminators are responsible for **disseminating** alerts in their own Member State and for **broadcasting** alerts and alert-related information to other Member States. Alert disseminators in an incoming alert postbox **acknowledge receipt** of alerts and are responsible for the initial dissemination of the alert to alert coordinators and alert authorities in their country. Alert disseminators in other alert coordinators decide which **additional authorities** in their region or field of competence should receive the alert.

Alert disseminators can **broadcast** new alerts to other Member States. They can also submit and broadcast additional information related to open alerts, including objections to closure or broadcast the withdrawal of an alert and closure proposals.

If the alert coordinator is given **'final approval'**, its alert disseminators are able to **edit the content** of alerts and alert-related information before broadcast. This setting also allows alert disseminators to **delete** the alert or alert-related information prior to broadcast.

6.2.3.4. Combined roles

IMI allows users to have combined roles. Thus, a user in an alert coordinator who has alert disseminator rights could also have rights as an alert handler. This would allow him to **initiate, submit and broadcast alerts**.

[3] If several users have local data administrator rights, all are given all user rights for alerts.

However, it should be borne in mind that submission and broadcast remain **separate steps**, which need to be completed individually, even if they are taken by the same person.

Differences between alert handlers and alert disseminators — Who can do what?

		Alert handler (in an alert authority or alert coordinator)	**Alert disseminator** (only available in alert coordinators)
Initiate an alert	Submit	✓	
	Broadcast		✓
Add additional information, including request for information and objections to closure	Submit	✓	✓
	Broadcast		✓
Withdraw an alert (initiating authority and coordinator only)	Submit	✓	
	Broadcast		✓
Propose closure of an alert (in MSE only)	Submit	✓	
	Comment	✓	✓
	Broadcast		✓
Close an alert (coordinator that broadcasts closure proposal only)			✓

6.3. Handling alerts in IMI

Alerts have a clearly defined **lifecycle** consisting of a number of basic steps and additional optional steps for some cases. As the alert moves from one step to the next, its **status** is automatically updated and displayed on the screen.

6.3.1. Sending an alert

6.3.1.1. Initiate and submit an alert

In order to initiate an alert, users need to be alert handlers in an alert authority or in an alert coordinator. As a first step, the alert handler has to complete a **checklist** of criteria for sending an alert (for details about these criteria, see the Guidelines on the alert mechanism available on the IMI website). IMI automatically leads him through this process. If all criteria are fulfilled, he enters the **data of the service provider** causing the potential danger and a **description of the case**. He can also add attachments. From the list of coordinators linked to his authority, he **chooses the alert coordinator** that will be responsible for broadcasting the alert. He **selects the Member State(s)** to which the alert should be sent. If he has information about individual authorities in the selected Member States that to his knowledge should be alerted, he can add this information in a free text field.

As soon as a draft of the alert is saved at any stage, the alert is assigned a **number**. Its status is:

'Draft Alert'

Once he has completed all steps, the alert handler submits the alert to the selected alert coordinator. The status of the alert changes to:

'Alert Submitted for Broadcast'

6.3.1.2. Broadcast an alert

All alert disseminators in the selected alert coordinator will be informed by automatic email that they have received an alert to broadcast.

If they think that their authority is not competent to decide whether the alert should be broadcast and that it should be sent to another alert coordinator, they can **forward** the alert to the other alert coordinator.

Once an alert disseminator has accepted the alert, the alert status changes to:

'Alert Awaiting Broadcast'

The alert disseminator should **check** whether all criteria have been fulfilled and whether the information is correct and complete.

If the alert coordinator has **'final approval'**, the alert disseminator can **edit the content** of the alert. With this setting, he can also **delete the alert** if he concludes that it should not be sent.

If this setting is not activated and an alert disseminator discovers, for example, that important information is missing, he can contact the alert authority outside IMI and ask it to amend the alert. If he concludes that the alert should not be sent at all, he can ask the authority to delete it.

Regardless of whether he has the 'final approval' setting, the alert disseminator can always **add recipient Member States** to the alert if, to his knowledge, it is necessary because the risk could exist in those Member States.

Once the alert disseminator is convinced that the alert is ready to be sent, he **broadcasts** it to the selected Member State(s). Each alert is also sent to the Commission automatically, as laid down in the Services Directive.

The alert receives the status: **'Alert is Broadcast'**.

6.3.2. Editing and rectifying an alert

After an alert has been broadcast, only the initiating Member State can edit or correct information contained in the alert. If it receives new information about the subject matter, it can:

- add a **recipient Member State**,
- change the **Member State of establishment** of the service provider,[4]
- change the **service provider details** and
- change the **case description**.

Adding a recipient Member State and changing the Member State of establishment can only be performed by the alert coordinator that broadcast the alert. If this alert coordinator has 'final approval', it can also change the service provider details and the case description; otherwise the initiating alert authority retains this right.

The changes are **automatically applied** to the alert and are **immediately visible** to all recipients. A new broadcast is not necessary.

If the Member State of establishment has been changed, all recipients of the alert will be informed in an automatic email.

6.3.3. Withdrawing an alert

Despite the built-in safeguards, a Member State may still have sent an alert on the basis of information or evidence that was wrongful or inaccurate, and may discover the error only at a later stage. If it becomes clear this is the case, the initiating Member State should **withdraw** the alert. This is possible at any stage of the alert lifecycle. Like sending an alert, withdrawing it is a two-step process. The initiating authority **submits a proposal to withdraw** the alert, which moves into the status **'Withdrawal to Broadcast'**.

The alert coordinator **broadcasts the withdrawal** (the 'Broadcast' button can be found via the tab **'Withdrawal Management'**). From that point onwards, the alert is no longer active. No new information can be added, and only a reduced view of the alert remains visible to recipients. The status of the alert is **'Alert Withdrawn'**.

6.3.4. Managing recipients of an alert

6.3.4.1. Acknowledge receipt of an alert

Alerts that are broadcast arrive in the incoming alert postbox of each Member State that is selected as a recipient and at the European Commission.[5]

It is the task of alert disseminators in an incoming alert postbox to **acknowledge receipt** of incoming alerts. They are informed in an automatic email when a new alert has arrived and will find it with the status **'Alert Awaiting Acknowledgement'**.

6.3.4.2. Disseminate an alert

Alert disseminators are responsible for the **first dissemination** of an incoming alert in the incoming alert postbox. They select the alert coordinators and alert authorities for whom the alert is relevant and disseminate it to them.

[4] This is only possible for as long as there is no closure proposal pending.

[5] For data protection reasons, the Commission cannot see any personal data contained in an alert.

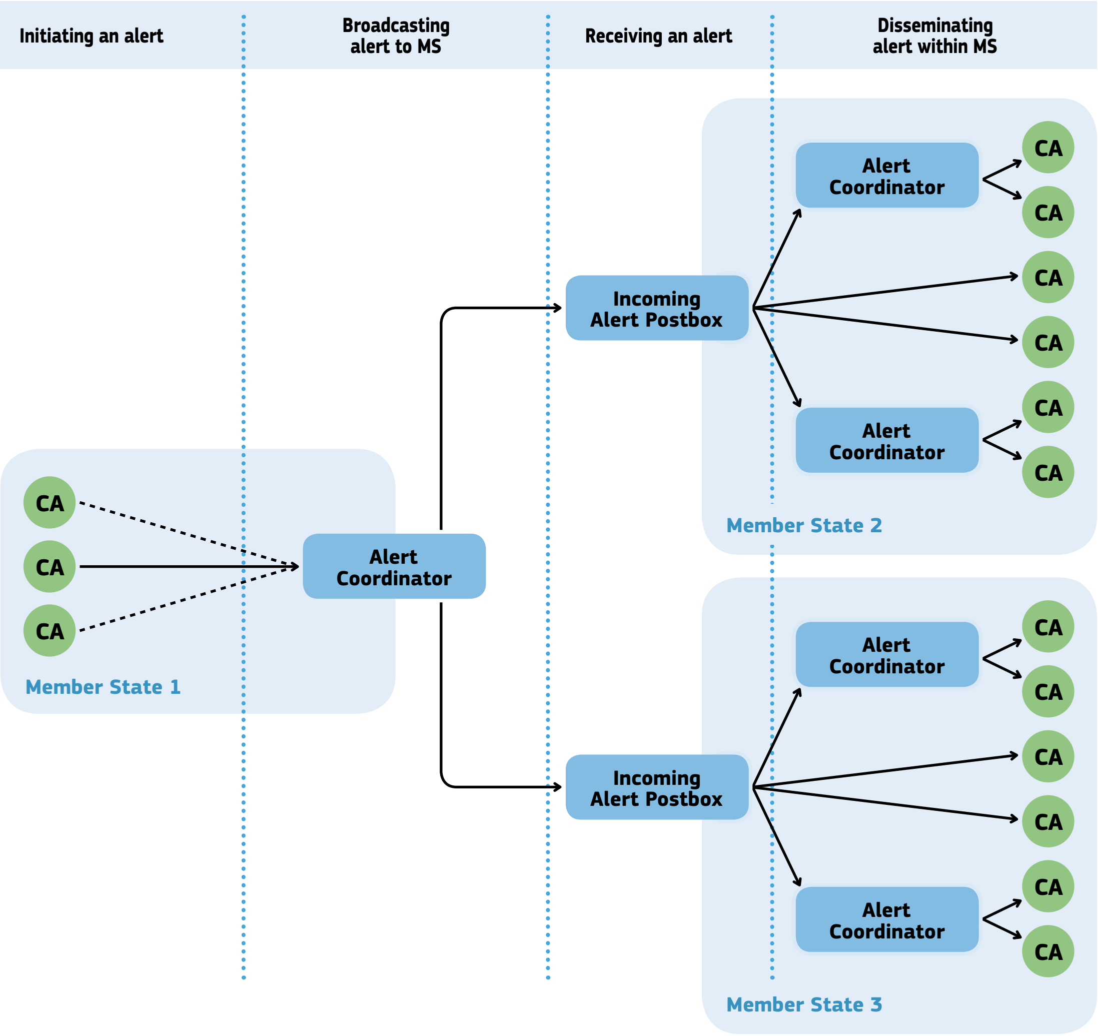
If the initiating Member State has **suggested authorities** to whom, to their knowledge, the alert should be sent, the alert disseminators check this and, if they agree, include these authorities in the list of recipients.

Alert disseminators in the selected alert coordinators can then **add further recipients**.

Once an alert has been disseminated, only alert disseminators in incoming alert postboxes can **remove recipients**. Recipients can only be removed if they have not yet taken any action on the alert. This could happen if a recipient finds that an alert is not relevant for his authority and informs the incoming alert postbox. If the authority is removed from the list of recipients, it will not receive information about any of the subsequent steps in the lifecycle of the alert.

Note that **dissemination** also takes place **in the Member State that initiated the alert**. The incoming alert postbox in that Member State automatically receives all outgoing alerts. Once an alert has been broadcast, the incoming alert postbox in the initiating Member State can select **additional recipients** in its country and disseminate the alert to them.

Sending and receiving an alert



6.3.5. Adding additional information on an alert

At any point of the lifecycle of an alert, any Member State involved in the alert can **add information** to it, e.g. to inform the other recipient Member States about measures it has taken against the service provider in question. Similarly, recipient Member States can ask for clarification from the initiating Member State or from another recipient Member State that contributed information to the alert previously. The additional information function can also be used to suggest to the Member State responsible for closure that the alert be closed.

Both sending and requesting additional information is a **two-step process**. An alert handler or alert disseminator submits the information to an alert coordinator, and an alert disseminator in the alert coordinator checks and broadcasts it.

All alert handlers and alert disseminators in all authorities involved in the alert will be informed in an automatic email that new information has been added to the alert.

6.3.6. Closing an alert

As explained in the alert guidelines, the **Member State in which the service provider is established** is responsible for launching the closure process. This should happen as soon as the risk is eliminated.

If the Member State of establishment (MSE) is **unknown**, the Member State that initiated the alert is responsible for the closure process.

There are two stages to the closure process:

- First, all authorities in the MSE have the chance to agree on whether closure should be proposed (= **comment period**).
- Second, after the closure proposal is broadcast, all other Member States involved have the chance to object to closure if they consider that the alert should remain active (= **objection period**).

6.3.6.1. Propose closure of an alert

Alert handlers in any recipient authority in the MSE can **propose closure of the alert** if they establish that the risk no longer exists. The closure proposal can be submitted to any coordinator linked to the authority, who then becomes the **'closing coordinator'**.

As soon as they **submit the proposal** (unless any action is taken by the closing coordinator), all other authorities that received the alert in the MSE are informed by automatic email that they can add comments to the closure proposal. If the closing coordinator has final approval, it can edit or delete the closure proposal at any time.

Note that, as the comment stage only involves one Member State, there is no need for a two-step process involving the alert coordinator at this stage.

The status of the alert changes to **'Closure Proposal Open for Comments'**.

6.3.6.2. Comment on a closure proposal

The closure proposal remains **open for comments** within the MSE for a set period of time, agreed upon by all Member States. During this time, the proposal can still be **edited or cancelled**, either by the alert authority that submitted it or by the closing coordinator (depending on the 'final approval' setting).

At the end of the comment period, the alert disseminators in the closing coordinator are informed by email that the comment period has expired. From this point, no further comments can be added. However, the closure proposal itself can still be edited or cancelled. The status of the alert changes to 'Closure Proposal Awaiting Broadcast'.

6.3.6.3. Broadcast a closure proposal

An alert disseminator in the closing coordinator then **assesses all comments** received and, on this basis, decides whether or not the closure proposal should be broadcast to the other Member States.

If he concludes that the alert should remain active, he can **cancel the closure proposal** (if the alert coordinator to which he belongs has final approval) or ask the authority that initiated the closure proposal to cancel it.

If he concludes that the alert should be closed, he **broadcasts the proposal** (the 'Broadcast' button can be found under the tab **'Closure Management'**). He can choose to **include certain comments or all comments** received in his Member State with the proposal. The broadcast generates an automatic email to all alert handlers and alert disseminators that received the alert in all Member States involved, informing them that closure has been proposed. The alert status changes to **'Closure Proposal Open for Objections'**.

6.3.6.4. Object to a closure proposal

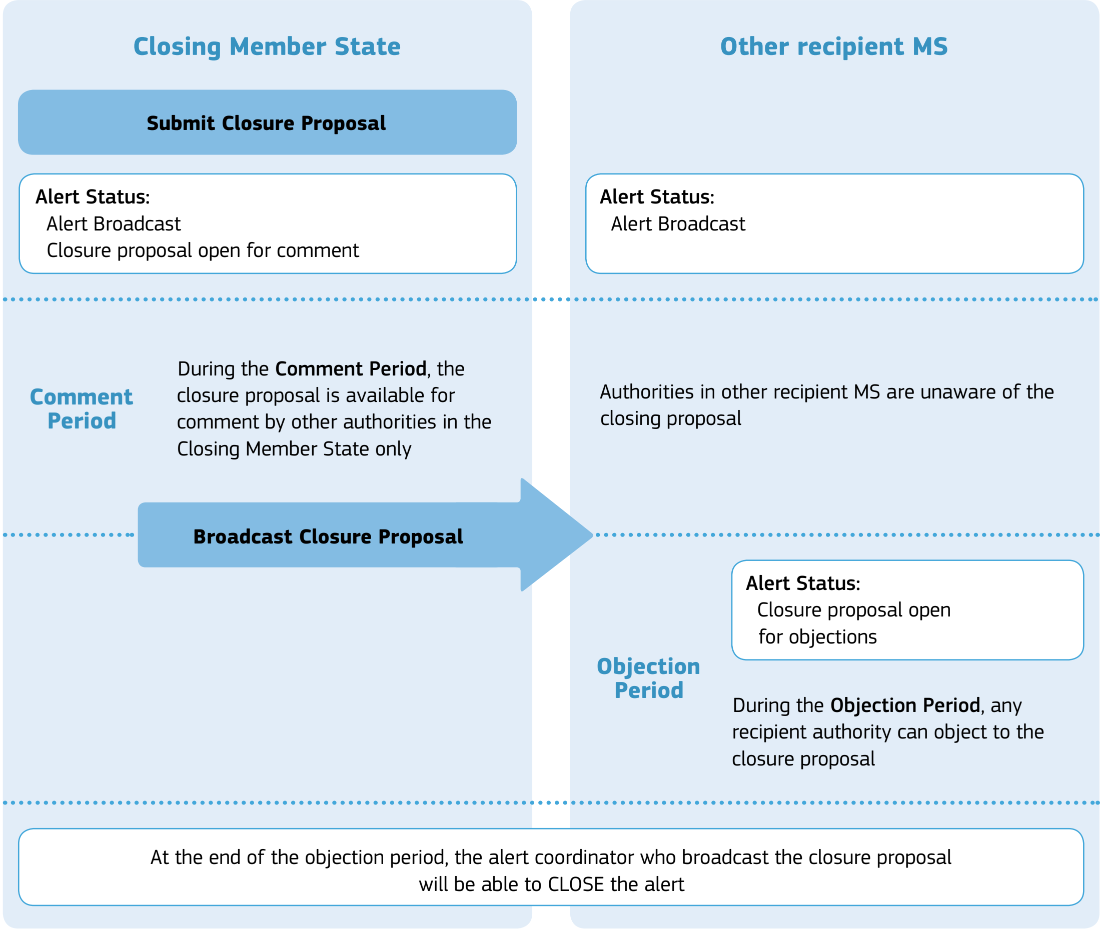
All other Member States now have the chance to raise any **objections** they may have against closing the alert, provided that they have information showing the risk persists.

The time frame for lodging objections is also set by agreement with all Member States. Within this period, alert handlers and alert disseminators in alert authorities and alert coordinators can **submit objections** to an alert coordinator. They can do this **via the 'Additional Information' function**, which contains a heading 'Objection to a closure proposal'.

The submission and broadcast of objections is a **two-step process**, just like sending any other type of additional information. An alert disseminator in an alert coordinator decides whether or not the objection should be **broadcast** to other Member States. Once it is broadcast, all recipients of the alert in all Member States are informed of the objection by automatic email.

When the objection period expires, the alert disseminators in the closing coordinator in the MSE are informed by automatic email.

The comment and objection periods



Closing Member State

Other recipient MS

Submit Closure Proposal

Alert Status:
Alert Broadcast
Closure proposal open for comment

Alert Status:
Alert Broadcast

Comment Period

During the **Comment Period**, the closure proposal is available for comment by other authorities in the Closing Member State only

Authorities in other recipient MS are unaware of the closing proposal

Broadcast Closure Proposal

Alert Status:
Closure proposal open for objections

Objection Period

During the **Objection Period**, any recipient authority can object to the closure proposal

At the end of the objection period, the alert coordinator who broadcast the closure proposal will be able to CLOSE the alert

6.3.6.5. Close an alert

Taking into account any objections made by other Member States, the closing coordinator in the MSE then decides whether the alert should be closed. In order to be able to **close an alert**, a user needs to be an alert disseminator in the closing coordinator.

The status of the alert changes to **'Alert Closed'**.

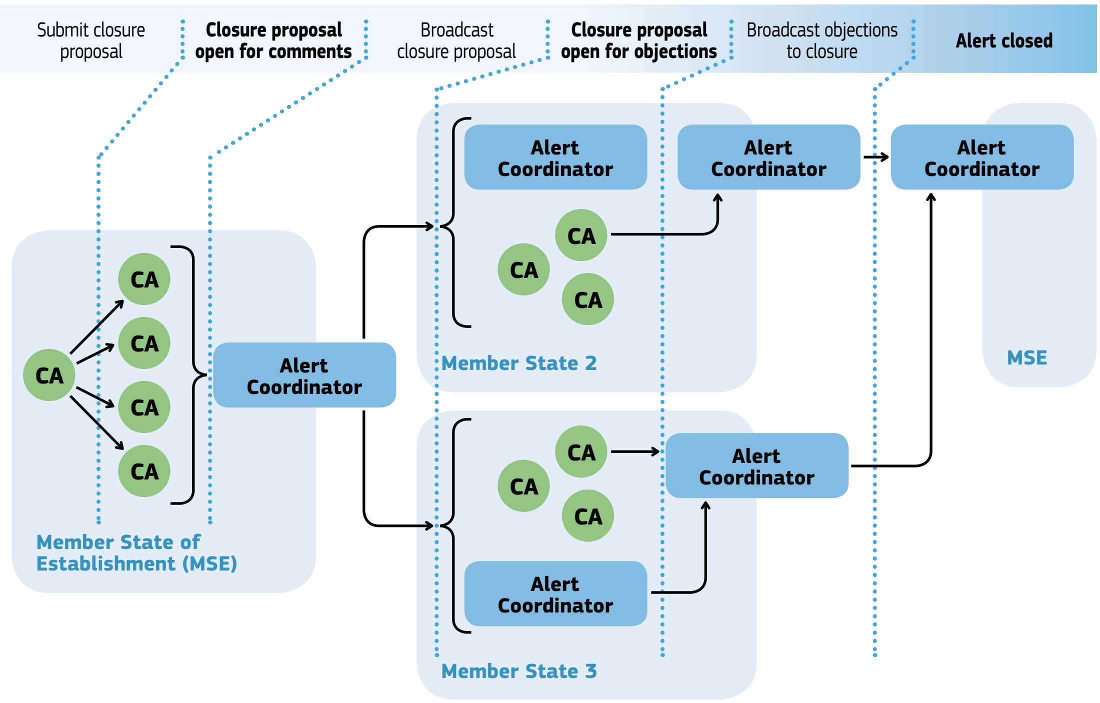
Once the alert has been closed, only limited details remain visible for all users. These include:

- an overview of the alert without any personal data,
- the list of recipients and
- the history of events.

Six months after closure, all personal data is automatically removed from the system.

If a Member State is convinced that the risk has still not been eliminated, despite the MSE closing alert, it can **launch a new alert**.

Closing an alert



6.4. Keeping track of alerts

6.4.1. Automatic emails

IMI sends automatically generated emails to all actors involved whenever they can **take action** on an alert or when **new information** is available. These emails are sent only to the individual email addresses of users with the right user profile for alerts. Therefore, it is important to frequently check the email addresses registered in IMI.

All emails are standardised and do not contain any information about the content of an alert or any personal data of the service provider concerned.

6.4.2. Searching for alerts

Each user with access to the alert workflow in IMI also has access to the list of alerts involving his authority. This list shows:

- Alert numbers
- The service activity concerned
- The Member State of establishment of the service provider concerned
- The authority that initiated the alert
- The current status of the alert and
- The broadcast date.

The list is **searchable** using various criteria. Depending on their user profile, users can open alerts from this list and take action on them.

6.4.3. Printing alerts

Alert authorities and coordinators may wish to **keep a record** of alerts sent and received through IMI. For this purpose, they can generate and print reports at any stage in the alert lifecycle, including when the alert is in draft status.

Any user can print alerts at the level of detail he is able to see. When an alert has been withdrawn or closed and only the reduced view remains visible, only this reduced view can be printed.

Please note that any further processing of printed data must comply with national and European data protection rules.

6.5. Further information on alerts

For more detailed information on alerts, including data protection safeguards and how to set up the structures within a Member State to deal with alerts, please see the Guidelines on the alert mechanism:

❯ **http://ec.europa.eu/internal_market/imi-net/docs/Alerts_EN.pdf**

7. Handling case-by-case derogation

(Art. 35 of the Services Directive)

This chapter deals with the technical aspects of handling case-by-case derogation in IMI, as provided for in Article 18 of the Services Directive.

You will find further guidelines on the conditions for using case-by-case derogation and potential case scenarios on the IMI website.

The Services Directive module of the Internal Market Information System (IMI) supports **two workflows**: one for standard information exchange and one for the alert mechanism. Access to each workflow is restricted to authorities that are specifically registered for it.

Case-by-case derogation is dealt with through the standard information exchange workflow. This means that an authority dealing with case-by-case derogation needs to be registered in IMI (1) for the Services Directive module and, within this module, (2) for standard information exchange.

Only specific functions of the case-by-case derogation workflow are described below. For general information about how to send and reply to requests, please see chapter 5.

The Services Directive provides for **two different procedures** to handle case-by-case derogation: the **'normal procedure'** and the **'urgency procedure'**.

7.1. The normal procedure (Article 35(2) to 35(5) of the Services Directive)

There are three steps in the normal procedure:

(1) The Member State in which the service is provided **sends a request** to the Member State in which the service provider is established (MSE) and asks it to take measures in relation to the provider.

To do this, select the menu option **'Create Request'** and the legislative area 'Services Directive'. Having selected the responding competent authority in the MSE, choose the question set **'Case-by-case Derogation Request to Member State of Establishment'**. Please read the explanations on screen carefully and follow them. IMI will lead you through a **checklist** of 10 steps, covering all conditions that need to be fulfilled to send the request. Before you can send the request, you must also fill in the **free text** fields to **describe the case** and a **justification** for why you are using case-by-case derogation.

(2) The MSE carries out the checks and replies to the request, indicating the measures it has taken or intends to take.

To do this, the responding authority **accepts the request** and **replies** to it. If the MSE does not intend to take any measures, the authority must **justify** this decision.

(3) If the requesting Member State is not satisfied with the measures taken by the MSE, it notifies the MSE and the Commission of the measures it intends to take.

In this case, the requesting authority chooses the question set **'Case-by-case Notification of Measures'**. It completes the **checklist** and fills in the required **free text** fields, stating why it considers the measures taken by the MSE to be inadequate or insufficient and why it believes that the measures it intends to take are justified and proportionate.

When the notification is sent, the Commission examines the case and, unless it adopts a decision to the contrary, the requesting Member State can take the notified measures 15 days after notification.

7.2. The urgency procedure (Article 35(6))

Where there is an imminent risk to the safety of services, the Member State in which the service is provided can **take measures immediately**, without consulting the MSE.

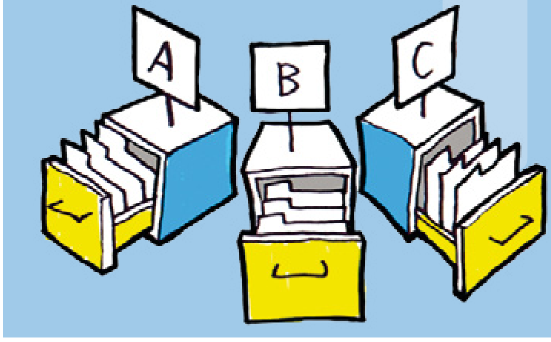
It must **notify these measures to the MSE** using the question set **'Case-by-case Notification of Measures'**. In technical terms, this notification works exactly like the notification under step (3) of the normal procedure.

7.3. Managing case-by-case derogation in IMI

Every authority in the Member States that has access to the information exchange workflow in the IMI module for the Services Directive also has access to the question sets for case-by-case derogation. However, the instructions displayed on screen make it very clear that case-by-case derogation is only to be used in exceptional circumstances.

Please note that step (3) of the normal procedure is not technically linked to steps (1) and (2). Technically, step (3) is a new request. This means that the authority that sent the request in step (1) does not necessarily have to be the one that sends the notification in step (3). Member States are thus **free to assign the corresponding responsibilities to different authorities**. However, in order to allow the parties involved to make the link with the preceding request, **the notification should contain a reference to the number of this request**.

8. The Registers Directory



This chapter deals with the directory of registers available in IMI. It explains how to add new registers to the directory, how to update the register information and how to consult the directory.

A database of register information has been developed in IMI to support the implementation of Article 28(7) of the Services Directive. This article states that Member States are obliged to make registers of service providers, available to competent authorities of other Member States.

The registers directory is not limited to registers concerning service providers. Information about **any register may be added** to the directory and **any IMI user can consult it**. The information about registers will enable authorities in other Member States to consult registers and find information they require in the context of administrative cooperation, which may avoid the need to send an information request.

8.1. Registers: who can do what?

The table below summarises user rights to view and maintain registers.

Action	Actor
View registers	All IMI users (can see all registers)
Add a register	Any LDA (of any authority)
Edit information (including the managing authority)	LDA of the managing authority
Delete a register from the directory	LDA of the managing authority

8.2. Adding a register

Any user with local data administrator rights (LDA) can add a register to the directory. You need to follow a sequence of steps to add a register, providing (1) general information, (2) access information, (3) register content and (4) authority information.

8.2.1. General information

First you need to enter some general information including the register name, an informal title, geographic coverage, the type and nature of the register (categories) and the languages in which register information is provided. Free text can be added to further explain any piece of information.

Providing an informal title for the register

The purpose of the informal title is to help users identify the correct register when they search the register database. The informal title should clearly convey the nature of the register; it should be reasonably short and should not be an abbreviation. If the official register name is sufficiently clear and descriptive, the same name may be entered for the informal title. It is called the informal title because it is translated into all official EU languages by the European Commission without formal verification by the Member States.

Register type

Registers are grouped into two main types, general and activity-specific. General registers contain information that does not relate to a particular economic activity, such as a company register or an insolvency register. Activity-specific registers contain information relating to particular areas of economic activity, and usually to specific services and/or professions. Depending on the type of register selected, different lists of register categories are offered. A careful selection of register categories will improve the quality of search results for users in other Member States.

Geographic coverage

The geographic coverage of a register may be national, regional or local. For regional and local registers of countries defined in IMI as regional countries, you must select one of the pre-defined lists of regions. For regional or local registers of countries that are not defined as having a regional structure in IMI, the region or area concerned should be included in the 'register informal title'.

8.2.2. Access information

The next two steps require you to enter information about access to the register including on-line availability, direct links to on-line registers, access restrictions and payment requirements. If a register is available on-line, you must provide at least one link to the register. For each link, you must specify the language of the linked website.

8.2.3. Content information

The two next steps require you to enter information about the content of the register, including types of information contained in the register, the use of register information, verification and maintenance of register information, and whether registration is mandatory.

8.2.4. Authority information

The final steps in adding a register concern the two authorities associated with the register, the owner and the manager.

Owner Authority

This is the authority or body responsible for the register content. The owner may or may not be registered as an IMI authority. A user may add a register owned by his authority or may add a register on behalf of another authority.

Managing Authority

By default the managing authority is the authority that adds a register to the IMI database. This authority retains the right to edit or delete the register from IMI. When adding a register, the user's authority is displayed as the managing authority and cannot be changed. Once the register has been added, the right to manage a register can be transferred to another IMI authority (see 8.4 below).

8.3. Updating register information and deleting registers

Only a local data administrator in the managing authority can update information about the register or delete the register. All register information described above can be updated, including the managing authority. When a register is deleted, an automatic email notifies all LDAs in the managing authority.

8.4. Transferring the right to manage a register to another authority

A local data administrator of the managing authority of a register can edit any data, including owner and managing authority information. If the managing authority is changed to a different authority, an automatic email notifies the LDAs in the new managing authority that they are responsible for the register information in IMI. If an LDA changes the managing authority, he will no longer have the right to edit or delete the register.

8.5. Consulting registers in IMI

Registers can be consulted via two search menu options. Individual registers can be selected and viewed from the results list. All IMI users have access to the register search and can view register information. When you view a register you will get access to edit and delete functions if you have these user rights.

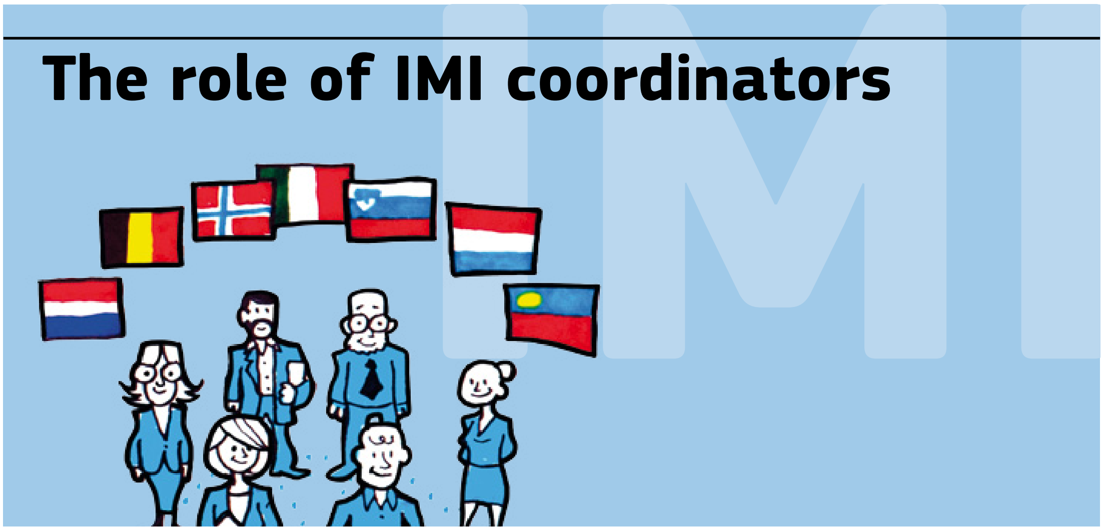
8.5.1. Quick search

The quick search allows you to search for registers by selecting a country and inserting some free text. The free text search is performed on the registers' official names, informal titles, register type, geographic region, register categories and the selected 'types of information contained in the register'. If more than one word is entered in the free text box, the search will find registers with a match on all words. The search is performed in the language in which the screen is displayed and will return matches on words that are spelt like or sound like those entered.

8.5.2. Advanced search

This search allows you to specify search criteria by selecting from drop-down lists. You can also search register names and authority names. The relationship between the different criteria is an 'AND' relationship, i.e. a register will be found if all criteria are met. Some advanced criteria are provided to help you manage the directory.

9. The role of IMI coordinators



This chapter describes the administrative, support and content-related tasks of IMI coordinators. It explains how data administrators in a coordinator can register and validate an authority in IMI. It also presents the settings that dictate what an authority can do in the system and how to manage them.

IMI coordinators play an important role in the set-up and ongoing operation of IMI. They have (1) an **administrative function**, (2) a **support function** and (3) a **content-related coordination function**. In addition, IMI coordinators may also act as competent authorities and may be involved in, for example, information requests as described in chapter 5.

9.1. Administrative function

The administrative tasks in IMI mainly involve registering and/or authenticating other authorities and managing accesses to legislative areas and workflows.

❯ User role: data administrator

Each authority registered in IMI with a coordinator role must have at least one user with data administrator rights. This allows the coordinator to execute tasks required by its administrative function in IMI.

A data administrator is responsible for managing the data of the authorities he or she coordinates (in contrast to a local data administrator, who is responsible for managing his own authority's data). He or she has the right to register, invite and manage other authorities in IMI in the corresponding legislative area. Data administrators of an access coordinator can update legislative and workflow settings of coordinated authorities.

Data administrators can also register additional users, manage user rights and reset the password of users in a competent authority for which they are the validating or access coordinator.

9.1.1. Administrative roles in IMI

Two types of coordinator have horizontal competence in IMI and therefore have access to **all legislative areas and workflows** by default. These are:

> **National IMI coordinator (NIMIC):** an authority that oversees the overall deployment and smooth functioning of IMI at **national level**. NIMICs can register and validate any other type of authority and manage access to any legislative area and workflow in the system.

> **Super-delegated IMI coordinator (SDIMIC):** Member States with a federal structure may designate authorities with **overall responsibility for IMI in one region**. An SDIMIC can carry out the same functions as a NIMIC, except it cannot register other SDIMICs.

All other authorities registered in IMI have access to at least one legislative area and related workflow. Authority roles are defined separately for each legislative area and then for each workflow available within a legislative area. The following roles are available in a **legislative area**:

> **Legislative area IMI Coordinator (LIMIC):** This is a coordinator with **overall competence for one legislative area**.

Administrative functions of IMI coordinators

		NIMIC	SDIMIC	LIMIC	DIMIC
General administrative role: 'Validating coordinator'					
Can register/validate SDIMICs		✓			
Can register/validate LIMICs		✓	✓*		
Can register/validate DIMICs		✓	✓	✓	
Can register/validate CAs		✓	✓	✓	✓
Administrative role per legislative area: 'Access coordinator'					
Can manage legislative area and workflow access for SDIMICs		✓			
Can manage legislative area and workflow access for LIMICs		✓	✓		
Can manage legislative area and workflow access for DIMICs		✓	✓	✓	
Can manage legislative area and workflow access for CAs		✓	✓	✓	✓
Requests workflow	Can assign the role of Authority (Requests)	✓	✓	✓	✓
	Can assign the role of Request Coordinator	✓	✓	✓	✓
Alerts workflow	Can assign the role of Alert Authority	✓	✓	✓**	✓
	Can assign the role of Alert Coordinator	✓	✓	✓**	
	Can assign the role of Incoming Alert Postbox	✓	✓	✓**	

(*) Only one LIMIC per legislative area in the region for which the SDIMIC is responsible.
(**) Only if the LIMIC is responsible for the legislative area of services.

For each Member State there can be only one LIMIC per legislative area.[6] A LIMIC can register other authorities with the role of Delegated IMI coordinator (DIMIC) or competent authority in the legislative area for which it is responsible and it can manage their access to that legislative area and related workflows.

> **A delegated IMI coordinator (DIMIC)** is usually responsible for one or more legislative area(s) in a geographical area or in relation to a particular area of competence in a legislative area. A DIMIC can register and validate other authorities with the role of competent authority in the legislative area(s) for which it is responsible.

> **A competent authority** can have access to any of the workflows available in the legislative area to which it has access. A competent authority cannot register other authorities or manage access to legislative areas.

Please note that an authority may have different roles in different legislative areas. For example, a Ministry of Economy can be a DIMIC for the legislative area of Services, and be a competent authority in the Professional Qualifications module of IMI.

Regardless of their legislative area role, IMI coordinators may have one or both of the following administrative roles:

- **Validating coordinator**, the coordinator that registers and/or validates an authority in IMI and is responsible for this authority's data management. Data administrator(s) of the validating coordinator can:
  - Manage the authority's name, informal title, languages, contact email address (to which most of the automatic emails generated by the IMI system are sent) and contact details;

[6] Exceptionally, in Member States with a federal structure, SDIMICs can register one LIMIC per region.

- Manage the areas of competence by adding/removing policy area(s) or area(s) of economic activities;
- Manage users of the coordinated authority, including adding and removing users;
- Manage the authority's access to the system (see more details about the authority lifecycle in chapter 9.1.5).

- **Access coordinator**, the coordinator responsible for granting and managing an authority's access to a particular legislative area and workflow. In addition, data administrator(s) of an access coordinator can:

  - Edit the authority's general data for the legislative area (keywords, professions, linked authorities);
  - Manage users in the coordinated authority, including adding and removing users;
  - Define the workflow-related settings (or 'flags');
  - Define and, if necessary, change the workflow role for the coordinated authority;
  - Link other coordinators to the authority for content-related intervention in each workflow to which the authority has access.

9.1.2. Registering a competent authority in IMI

9.1.2.1. Before registration

IMI coordinators are responsible for **identifying the competent authorities** that should use IMI for one or more legislative areas. Before registering an authority in IMI, the coordinator needs to **contact the authority** and ask for their general contact information, including the authority's official name, telephone number, address and website. He must also ask for the name and email address of the person who will be registered as the first user of the authority.

9.1.2.2. Registration: important aspects

To register a new authority, you have to fill in a number of fields covering basic descriptive data about the authority, its access to legislative areas and workflows and details of the first user. The registration process is very similar to the one described in chapter 3.1.2.2. Chapter 4.2 provides more details about authority descriptive data and chapter 9.1.4 explains the workflow settings that the coordinator needs to choose when registering.

The information entered in IMI about each new authority should be **up-to-date and correct**. This is particularly important for the email address of the first user, as this is where the system will send the temporary password which allows the user to log in to IMI.

You will also have to decide to which legislative area(s) and workflow(s) the new authority will have **access** and with what **role** (see chapter 9.1 for legislative area roles and chapters 5.2 and 6.2 for workflow roles).

When the workflow role is 'authority', for each workflow and legislative area to which the new authority is given access, you will also have to define **at least one linked coordinator**, i.e. the coordinator that can be involved in information exchange (e.g. request or alert). You can link different coordinators for different legislative areas, and have more than one coordinator for the same workflow. Once the authority is registered, you can update their linked coordinators if necessary.

By default, the coordinator who registers the authority becomes the authority's validating coordinator, as well as access coordinator for all legislative areas to which the authority is granted access. Once registration is completed, you will be able to change your role as validating or access coordinator and give this role to other coordinators in your Member State. If you register an IMI coordinator, then the coordinator responsible for managing its data or access must be of a higher level (e.g. for a DIMIC, it has to be a LIMIC, SDIMIC or a NIMIC).

❯

Registration of IMI coordinators

The procedure for registering an IMI coordinator is essentially the same as for a competent authority. A specific **naming convention** should be used for national and super-delegated coordinators, whose name always includes the abbreviation '(NIMIC)' or '(SDIMIC)'. For SDIMICs, the name should also include the region for which this coordinator in responsible. For example: ***Innenministerium Baden-Württemberg (SDIMIC)***.

For each workflow the new coordinator is given access to, you will also have to define several coordinator-specific settings (or flags). These are explained in chapter 9.1.4.2.

9.1.2.3. After registration

The IMI system will automatically propose a username for the first user in the authority you are registering. It is your responsibility to **give this first user his username**.

You will have to do this outside of the IMI system using whatever method is most secure and appropriate to the circumstances (telephone, encrypted email, or in person). It is essential that you do not forget to communicate the username to the first user in the authority. But you should never send the username by email to the same email address which has been registered in IMI for the user.

Within 48 hours, a temporary password will be sent automatically by the IMI system to the user's email address. You will not see this password. Once the new user has both his username and temporary password, he can access IMI.

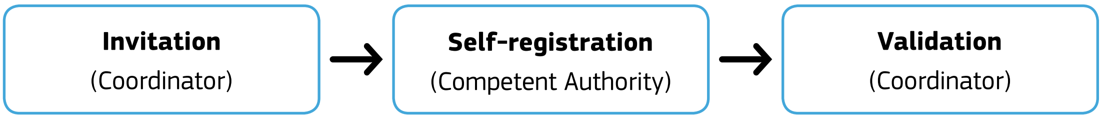
❯

> **Keep in contact with coordinated authorities**
>
> When you contact the first user of the authority, encourage him to log on to the system as soon as he receives his temporary password. The first user is responsible for checking the authority data and registering additional users (at least one other user). It is recommended that IMI coordinators contact their new authorities again to ensure the first user has received his password and has successfully logged on to IMI.

9.1.3. Self-registration: guidelines for IMI coordinators

This section focuses on the actions you need to take if you are an IMI coordinator and decide to invite a new authority to register in IMI.

There are three steps in the self-registration process for competent authorities. First, the coordinator creates and submits the invitation to register. Second, having received the invitation, the competent authority registers its data in the system (self-registration proper). Thirdly, the coordinator validates the data entered by the authority.



Invitation
(Coordinator)

→

Self-registration
(Competent Authority)

→

Validation
(Coordinator)

9.1.3.1. Managing invitations to register

Self-registration upon invitation reduces the workload of IMI coordinators while allowing them to keep overall control of the process. It also ensures that only relevant competent authorities self-register in IMI, and for the appropriate legislative areas and workflows.

Depending on the number of authorities you intend to invite to register in IMI, you may choose to create invitations individually or in groups.

- **Creating a draft invitation**

  For each invitation to register in IMI, you will need to provide the following details:

  > **a valid email address** for the authority;

  > **a name** for the authority (not necessarily its official name, as this is just a name that will be displayed in your list of invitations);

  > **the legislative area(s) and related workflow(s)** for which you are inviting the authority to register in IMI;

  > **optionally**, you may enter a **personalised message** to be included in the invitation email sent to the authority. You may, for instance, use this message to give specific instructions about the authority's informal title or about the self-registration process in general.

  Each invitation will be saved as a draft and kept in a list of **draft invitations**. You can **edit** your draft invitations at any time, and **submit** them either one by one or in groups.

- **Creating multiple invitations — draft bulk invitations**

  The system also allows you to create several invitations at the same time ('bulk invitations'). To do so, you need to take the following steps:

> Export the **template file** provided in IMI by right-clicking on the Excel icon displayed on the 'Create Invitations' screen.

> In this file, record a **name** and a **valid email address** for each authority to be invited to register. When working with this file, please make sure you **do not change its format**. This is particularly important if you are importing lists into the template file. At the end, do not forget to save the changes you made to the file.

> Upload the file with invitations. The invitations imported from your file will be displayed in your list of **draft invitations**.

Draft invitations created using the bulk function will not include any legislative area/workflow. The coordinator has to **edit** the draft invitations and select the relevant legislative area(s) and workflow(s). Draft invitations can be edited one by one or by specifying bulk changes to a group of invitations (see section below).

- **Making bulk changes to draft invitations**

The system allows you to edit a number of invitations at the same time. Bulk changes (i.e. changes to all or selected invitations) can be useful when you have a large number of draft invitations, most probably after you have used the template file to create the invitations. These changes could be adding personalised text or selecting the legislative area(s) and workflow(s) for which the authorities concerned should register.

Please note that the alerts workflow for the legislative area of services cannot be selected when making bulk changes. To invite an authority that needs to have access to this specific workflow, you will have to edit the related invitation individually.

9.1.3.2. Invitation lifecycle: the typical flow

An invitation to register is always created with the status 'Draft' and typically passes through the following statuses:

- **Invitation Submitted**

The invitation remains in the status 'Draft' until the Coordinator confirms that it should be sent to the authority. At this point, the status changes to 'Invitation Submitted'. However, the invitation is not immediately sent to the competent authority.

> An invitation submitted **before 10am** will be sent to the authority **overnight**.

> An invitation submitted **after 10am** will be sent to the authority during **the night of the following working day**. This means that invitations submitted after 10am on a Friday will only be sent the following Monday night.

- **Invitation Sent Awaiting Registration**

Once sent, the invitation is assigned the status 'Sent Awaiting Registration'. The invitation consists of an email sent to the authority, inviting it to register in IMI (see chapter 3.1.2 of this document).

- **Registered Awaiting Validation**

Once the authority has completed self-registration, the invitation will automatically be updated with the status 'Registered Awaiting Validation'. In parallel, the inviting coordinator will receive an email informing it that the authority should be validated in IMI.

- **Authority Validated**

After you validate a competent authority that has registered in the system, the invitation will remain in your list of invitations for three months, with the status 'Authority Validated'.

9.1.3.3. Invitation lifecycle: alternative flows and statuses

An invitation to register may follow alternative paths which set new statuses for the invitation. Depending on the status, coordinators will be able to edit, withdraw or re-submit an invitation.

- **Invitation Rejected**

An invitation to register may be rejected for three possible reasons:

> **Duplicate email address:** The authority's email address in your invitation is registered in IMI for an existing authority or an invitation to register has already been created using the same email address;

> **Invalid email address:** The format of the email address is not valid.

> **No workflow selected:** The system will reject invitations that you create using the bulk invitations function and for which you did not select at least one workflow before submitting them.

When you submit the invitations to register, the system will immediately inform you of the number of invitations submitted and how many, if any, were rejected. For each rejected invitation you will be given a reason for the rejection and you will be able to edit the invitation accordingly (e.g. correcting the email address or entering another one). Then you can re-submit the invitations.

You can also make **bulk changes** to edit rejected invitations.

- **Invitation Blocked**

  If you submit 100 or more invitations on the same day, they will be blocked by the system for security reasons. They will be shown in your list with the status 'Blocked'.

  A European Commission IMI Administrator will contact you and ask you to confirm that you have intentionally submitted so many invitations to register. Upon your confirmation, the IMI Administrator will release the invitations to be sent overnight, and assign the status 'Sent Awaiting Registration'.

  If you submit one or more invitations by mistake, you may contact the IMI Helpdesk at the Commission and ask for them to be blocked. Please note, however, that this is only possible while an invitation has the status 'Submitted' (not 'Sent Awaiting Registration').

- **Invitation Expired**

  Each invitation includes a unique registration code which is only valid for 30 days. If the invited competent authority does not register before the expiry of the registration code, then the invitation is assigned the status 'Invitation Expired'. At this stage, the coordinator may **re-submit** the invitation.

- **Invitation Withdrawn**

  The inviting coordinator can withdraw an invitation with the status 'Sent Awaiting Registration' or 'Invitation Expired'. A withdrawn invitation will remain in the list of invitations for a period of three months, after which it will be automatically deleted. Withdrawn invitations can also be deleted manually before the end of the three-month retention period.

- **Validation Refused**

  If a coordinator refuses to validate the authority's registration in IMI, the invitation to register is set to the status 'Validation Refused'. After six months, it will automatically be deleted from the system.

9.1.3.4. Validating registrations

You will be notified by email when a competent authority that you invited to register in IMI has completed its registration. When you validate the authority's registration, the authority will become **active** in IMI and visible to IMI users searching for authorities in the system. As part of the validation, you can **check the authority's data** and edit it if necessary. You can also **set the legislative area and workflow access parameters**.

Following their self-registration, authorities will be assigned by default the role of competent authority at legislative area level and the role of authority at workflow level. If you would like to change any of these roles for the authority, you may do so before validating the authority's data.

9.1.4. Defining workflow settings

For each workflow to which an authority has access in IMI, a number of settings ('flags') have to be chosen. These flags influence the way an exchange of information is handled by an authority, giving a level of flexibility that reflects the different working methods of Member States and their authorities. These flags are first chosen **during the authority's registration in IMI**. Once the authority is registered, its access coordinator for the legislative area which supports the workflow can update them at any time.

9.1.4.1. Workflow settings for competent authorities

The three flags below are related to the **request workflow** of IMI. They **can only be changed by the coordinator**, not by the competent authority. Note that the replies to these questions can differ by legislative area for the same competent authority.

1. Is this authority **subject to approval** by the coordinator before sending requests or replying to information requests in this legislative area? (*DEFAULT VALUE = NO*).

   Some Member States will decide that certain competent authorities may only send and reply to IMI requests in a legislative area after the relevant IMI coordinator has approved them. The approval procedure is explained in chapter 5.3.7.

2. Is this authority exceptionally **allowed to refuse** a request from another Member State? (*DEFAULT VALUE = NO*).

   This setting determines whether or not a competent authority is entitled to refuse a request outright on behalf of its Member State. If a competent authority receives a request which it does not wish to accept (because it is not the correct competent authority) it can forward the request to another authority or to an IMI coordinator in its Member State, who should be able to identify the correct Responding Authority. In exceptional circumstances, however, a competent authority may be considered competent to refuse a request outright on behalf of its Member State.

3. Is this authority **allowed to accept incoming requests** from other Member States? (*DEFAULT VALUE = YES*).

   Certain competent authorities may be registered to use IMI and send requests to other Member States, but not to reply to requests from other Member States, in a particular legislative area. For example, a Member State may decide that its national Medical Chamber should reply to all requests from other Member States, but the regional Medical Chambers may create and send requests in their own names.

❯

Linking coordinators at workflow level

In addition to the ‘flag’ settings, each authority must be linked to at least one request coordinator for each legislative area to which they have access. When a coordinator registers a new authority, he or she will have to define the linked request coordinator(s) for the authority. If the authority registers itself, the validating coordinator will have to define the linked coordinator(s) upon the authority’s validation in IMI.

Following the authority’s registration or validation, its access coordinator for a specific legislative area or the local data administrator of the authority may add or change its linked coordinators as appropriate.

9.1.4.2. Workflow settings for coordinators

For the **request workflow**, the available flags are:

1. Does the coordinator **participate in ‘referral’** processes involving the authorities it coordinates? (DEFAULT VALUE = YES)

   As explained in chapter 5.3.6, IMI coordinators may get involved as referees if there is disagreement between authorities they coordinate and authorities in another Member State. A coordinator can decide whether or not to participate in referral processes for a legislative area.

2. Does the coordinator wish to **approve requests** from any of the authorities it coordinates before they are sent? (DEFAULT VALUE = NO)

3. Does the coordinator wish to **approve replies** from any of the authorities it coordinates before they are sent? (DEFAULT VALUE = NO)

   Please see chapter 5.3.7 for details on the approval procedure in IMI.

Following registration, an additional flag appears that can be changed by the IMI coordinator itself.

4. Does this authority **use the ‘allocation’ process** to allocate requests to its users? (DEFAULT VALUE = NO)?

   The implications of this flag are further explained in chapter 5.3.5.3.

For the **alerts workflow**, there is a **‘final approval’** flag for authorities with a coordinator role. This is explained in more detail in chapter 6.2.2.

When you register a coordinator in IMI, you may decide to select the default values for the flags above. The coordinator will be able to change any of these settings once it logs on to the system.

9.1.5. Managing the authority lifecycle, legislative area and workflow lifecycles

Each authority is assigned a status reflecting its rights to access and use IMI. In addition to its authority status, the system maintains an access status for each legislative area to which the authority has access or has requested access, as well as an access status for each workflow to which the authority has access or has requested access in a legislative area.

9.1.5.1. Authority statuses in IMI

- **Authority status: Registration requested**

  A competent authority that self-registers in IMI is assigned the status 'Registration Requested'. This means the authority is only visible to the data administrator(s) of the validating coordinator that issued the invitation.

- **Authority status: Active**

  A competent authority becomes 'Active' in IMI as soon as it is registered by an IMI coordinator or following validation of its self-registration by the validating coordinator. This means the authority may be granted access or it may request access to any of the legislative areas and workflows available in the system.

- **Authority status: Registration refused**

  In exceptional cases, the validating coordinator may refuse a competent authority's self-registration, in which case the authority's status is set to 'Registration Refused'. An authority with this status may still be validated by the coordinator for up to six months, after which the registration will be automatically deleted from the system.

- **Authority status: Suspended**

  A validating coordinator can remove a competent authority from IMI. This happens in steps, allowing the authority to finish any ongoing activity in the system.

  As a first step, the validating coordinator will suspend the authority's activity. To do this, the status of all workflows and legislative areas to which the authority has access must be set to the status 'Suspended' or 'Removed'.

  In the status 'Suspended', the authority can still participate in any ongoing information exchanges or alerts, but will not be able to send or receive new requests for information. Access to a new workflow or legislative area can no longer be requested or granted.

  Please note that it is possible to reactivate a suspended authority, in which case the authority status is reset to 'Active'.

- **Authority status: Inactive**

  Once all information exchanges concerning a competent authority in the status 'Suspended' have been closed, it is possible to remove access to all workflows and legislative areas to which the authority had access. The final step of the authority removal process is for the validating coordinator to set the authority's status to 'Inactive'. Six months later, the authority will be permanently removed from the system.

  In the meantime, the authority's users can still log on to IMI and new users can be registered. The authority can view its previous requests or alerts, but may no longer send or receive any new ones.

9.1.5.2. Legislative area access statuses

Access to at least one legislative area and at least one related workflow is granted to a competent authority upon registration or validation by the validating coordinator. In addition, a coordinator may at any time grant an active competent authority access to a legislative area and workflow to which it does not have access, or the authority itself can request access to a new area in IMI.

- **Legislative area access: Requested**

  When an authority requests access to a legislative area,[7] the data administrator(s) of the selected access coordinator can edit the authority's settings for the legislative area (e.g. update the list of keywords for the legislative area).

  The local data administrator(s) of the competent authority requesting access can also edit its data for the legislative area, but it can not yet send or receive requests/alerts in that legislative area.

- **Legislative area access: Active**

  When access to a legislative area is 'Active', the authority can register users and manage its data for this module of IMI. The authority can then be granted access or request access to any of the workflows available in that legislative area.

- **Legislative area access: Suspended**

  In exceptional cases, the access coordinator may decide to suspend an authority's access to a legislative area in IMI.[8] The coordinator may subsequently either reactivate or remove access to that legislative area.

[7] Access to a legislative area is also set to status 'Requested' following self-registration and before validation.

[8] Access to a legislative area for an authority with a coordinator role can only be suspended under very specific conditions. Should this be necessary in your Member State, please contact the Commission IMI helpdesk for assistance.

When the access status is 'Suspended', the competent authority can still handle its ongoing activities, but it can no longer send or receive new requests/alerts in the legislative area. The local data administrator of the competent authority can still register and manage users with access to the legislative area and may request that access be reactivated.

- **Legislative area access: Suspended (Reactivation requested)**

When the legislative area status is 'Suspended', the authority can ask its access coordinator to reactivate its access to the legislative area, provided that the authority status is 'Active'. Upon its request, the legislative area status becomes 'Suspended (Reactivation requested)'. If the coordinator decides to reactivate access, a 'Suspended' access is reset to 'Active'. If the coordinator rejects the authority's request for reactivation, the legislative area status remains 'Suspended'.

- **Legislative area access: Removed**

Once a competent authority with suspended access to a legislative area has closed all its ongoing requests/alerts in that legislative area, the access coordinator can remove the authority's access to the legislative area. Please note that this is possible only after the access to all workflows in that legislative area has been set to the status 'Removed'.

When access to the legislative area has been removed, the local data administrator of the authority may still request the reactivation of its access to the legislative area, provided that the authority status is 'Active'. The access coordinator may also decide to start the reactivation process for the legislative area.

- **Legislative area access: Removed (Reactivation requested)**

When the legislative area status is 'Removed', the authority can request its access coordinator to reactivate its access to the legislative area, provided that the authority status is 'Active'. Upon its request, the legislative area status becomes 'Removed (Reactivation requested)'. If the coordinator decides to reactivate access, a removed access is first reset to 'Suspended', and can only then be set back to 'Active'. If the coordinator rejects the authority request for reactivation, the legislative area status is reset to 'Removed'.

9.1.5.3. Workflow access statuses

- **Workflow access: Requested**

When an authority requests access to a new workflow,[9] the data administrator(s) of the selected access coordinator for that legislative area can edit the authority's settings for the workflow and define the coordinator(s) which will be linked to that authority at the level of the workflow. The coordinator may grant or refuse the requested access.

The local data administrator(s) of the competent authority requesting access can also edit its data for the workflow, but it cannot yet send or receive requests/alerts in that workflow.

- **Workflow access: Active**

When access to a workflow is active, the authority can register users and manage its data for this workflow. The authority can then send and receive information requests /alerts in the respective legislative area.

- **Workflow access: Suspended**

In exceptional cases, the access coordinator may decide to suspend an authority's access to a workflow in a legislative area.[10] The coordinator may subsequently either reactivate or remove access to that workflow.

When the workflow status is suspended, the competent authority can still handle ongoing activities, but it can no longer send or receive new requests/alerts within that workflow. The local data administrator of the competent authority can still register and manage users with access to the workflow and may request that access be reactivated. This can only be done if the access to the related legislative area is in the status 'Active'.

- **Workflow access: Suspended (Reactivation requested)**

When the workflow status is suspended, the authority can ask its access coordinator to reactivate its access to that workflow. If the coordinator decides to reactivate the access, then it is reset to 'Active'. If the coordinator rejects the authority's request for reactivation, the status returns to 'Suspended'.

- **Workflow access: Removed**

Once a competent authority with suspended access to a workflow has closed all its ongoing requests in that workflow, the access coordinator can remove the authority's access to the workflow.

[9] A workflow access is set to the status 'Requested' following self-registration and before validation.

[10] Workflow access for an authority with a coordinator role in that workflow can only be suspended under very specific conditions. Should this be necessary in your Member State, please contact the Commission IMI helpdesk for assistance.

When access has been removed, the local data administrator of the authority still has the option to request the reactivation of its access to the workflow.

- **Workflow access: Removed (Reactivation requested)**

When the workflow status is removed, the authority can ask its access coordinator to reactivate its access to the respective workflow, provided that its access in the related legislative area is active. If the coordinator decides to reactivate the access, the status 'Removed' is first reset to 'Suspended', and then reset to 'Active'. If the coordinator rejects the authority's request for reactivation, the workflow status returns to 'Removed'.

❯ Request access reactivation or authority reactivation

The authority status, legislative area status and workflow status of authorities registered in IMI are interrelated. In most cases, an authority can request access to a new legislative area or workflow or reactivation of its access to a legislative area or workflow. The general rules are:

> An authority may request access to a new legislative area or to a new workflow only if the authority's status is 'Active'.

> An authority may request reactivation of its access to a legislative area only if the authority's status is 'Active'.

> An authority may request reactivation of its access to a workflow only if its access to that legislative area is 'Active'.

9.1.6. Changing authority role

IMI allows you to change the roles of authorities registered in IMI. Depending on the status of the authority in the system and the distinction between administrative and content-related roles, IMI coordinators may change the role of an authority that they coordinate at the level of workflow or legislative area.

9.1.6.1. Change workflow role

An access coordinator may decide to change the workflow role of a coordinated authority. For instance, a Chamber of Crafts may have been initially registered as an authority for the requests workflow in the legislative area of services. This authority has competence at regional level, and therefore it could supervise other crafts authorities that only have local competence. The access coordinator of the regional Chamber of Crafts decides to give this authority the role of Request Coordinator, allowing it to participate in information exchanges with other authorities.

The workflow role of an authority that is already active in the system can only be changed when the workflow status is suspended. This change can be made by the access coordinator in that legislative area.

The workflow role can also be changed when the workflow access is in status 'Requested' or when the authority is in the status 'Registration Requested', i.e. before its registration in IMI is validated by the validating coordinator.

9.1.6.2. Change legislative area role

It is also possible to change the role of an IMI authority at the level of a legislative area. For example, a National IMI Coordinator may want to nominate as LIMIC for the legislative area of services an authority that is already registered in the system with the role of DIMIC for services.

To change an authority's role for a legislative area, its status in that legislative area must be set to 'Suspended'. Please note that in order to suspend access to a legislative area, the access coordinator first needs to suspend access to all workflows to which the authority has access in that legislative area.

For an authority that has just completed self-registration in IMI, the validating coordinator can change the authority role for a legislative area before validating its registration.

An authority role for a legislative area can also be changed when the related access is in the status 'Requested'.

9.2. Support function of coordinators

In addition to the above administrative role, IMI coordinators also play an important role in raising awareness of IMI, training users and ensuring that requests are dealt with in line with the legal obligations for administrative cooperation. This includes:

> Organising training for competent authorities;

> Providing IMI help and support facilities to users in their Member State;

> Assisting users in another Member State in identifying the right competent authority to contact on a particular topic (including forwarding requests to the appropriate competent authority);

> Raising awareness of IMI amongst authorities that may need to use it.

For training purposes, coordinators can use the IMI training system (an identical copy of the real IMI system without any real data), which can be accessed from the IMI website. NIMICs can provide coordinators with logins for trainers and trainees. The website also offers a wide range of training material and PowerPoint presentations, including a tailor-made training package for IMI newcomers. User guides, IMI brochures and small promotional items can be ordered by emailing markt-imi@ec.europa.eu.

9.3. Content-related coordination function

IMI coordinators also play an important content-related coordination function in relation to specific workflows within a legislative area. As IMI supports multiple legislative areas, it is possible that the provisions of a specific piece of internal market legislation give rise to a number of different workflows. For the Services Directive, for instance, IMI supports standard information exchange, a workflow for the alert mechanism and the case-by-case derogation.

In the standard information exchange, coordinators may get involved as referees if there is disagreement between competent authorities they coordinate and authorities in another Member State. They may also decide to approve requests from authorities they coordinate.

9.3.1. Content-related tasks of coordinators in the request workflow

9.3.1.1. Monitoring requests of coordinated authorities

IMI coordinators have an important role to play in ensuring that requests are answered in a timely manner. To ensure the smooth functioning of the system, coordinators should regularly **use the search facility for requests** to check that requests are sent and received by the authorities they coordinate. That way, coordinators will be aware of potential problematic situations (e.g. if an authority does not react to a new request in a reasonable time period) and can take appropriate action.

There may be several reasons why competent authorities do not deal with an incoming request in a timely manner. They may not be aware of the fact that a new request was sent to them, or they may not know how to deal with it. This is why it is important that a coordinator investigates the problem and helps the authority.

9.3.1.2. Intervening in a request between two authorities

The IMI system has a number of built-in safeguards to ensure adequate replies to IMI requests. For example, IMI coordinators can opt to intervene as referees in an information exchange between an authority under their coordination and an authority from another Member State (= **referral procedure**). This is explained in detail in chapter 5.3.6.

IMI coordinators may also decide to approve the requests sent by coordinated authorities or the responses they have provided to incoming requests (= **approval procedure**). This is explained in more detail in chapter 5.3.7.

It is important to note that **the IMI coordinator who intervenes in a request will never have access to any personal data** included in the request. The coordinator will be able to see certain details of the request, such as questions asked and any related answers, but he will not see any personal details about the subject matter.

9.3.2. Content-related tasks of coordinators in the alert workflow

IMI coordinators with access to the alert workflow in the legislative area of services have an important monitoring and intervention role in that workflow, too. **Alert coordinators** need to ensure that alerts submitted by authorities in their own country fulfil all the conditions and provide the right information before they are broadcast.

And alert coordinators, in particular those flagged as **incoming alert postbox**, need to ensure that alerts broadcast from other countries reach the correct recipients in their country. Alert coordinators in the **Member State of Establishment (MSE)** of the service provider concerned by an alert need to ensure that alerts are closed as soon as the risk of danger has been eliminated. For more details, see chapter 6.

9.4. Functionality for coordinators

- IMI coordinators with access to the request workflow can use **specific search criteria for requests** to monitor the flow of requests of authorities they coordinate. This allows them to identify potential problems and assist authorities in finding a suitable solution. IMI also allows request coordinators to display all requests where the coordinator plays a content-specific role (e.g. as part of the approval or referral process).
- Coordinators can also **send emails** to a list of competent authorities **through IMI**. By default, you can contact all authorities that you have registered or that you are linked to as a coordinator. You may also search the system to display all other competent authorities registered in IMI from your Member State.

  A number of pre-structured emails are available in the system. You can adapt these emails to your needs or draft your own email to reach all or a selection of authorities in your Member State simultaneously. This enables you, for instance, to ask all authorities recently registered in IMI to update the data about their authority. This function is available to users with 'data administrator' rights.
- To assist coordinators with the management of coordinated authorities, IMI allows users with 'data administrator' rights to **search for a competent authority by using the email address** of the authority or of one of its users.

10. IMI and data protection

This chapter briefly addresses the issue of data protection in IMI.

As IMI is used for the exchange of personal data, a high level of data protection is important. Relevant data protection legislation fully applies to IMI.[11] IMI helps to ensure compliance with this legislation because it provides a clear framework for what information can be exchanged, with whom and under what circumstances. Specific measures to ensure compliance with data protection rules have been built into IMI. IMI thus adds an additional layer of security — uncertain ad-hoc information exchanges between Member States by means of fax or e-mail or letter are replaced by a structured system that actively improves compliance with the security and data protection obligations.

For example, only competent authorities directly involved in an information exchange have access to personal data in IMI. In addition, any personal data contained in an information exchange is automatically deleted in the system at the latest six months after the formal closure of the information exchange.

On 29 August 2011, the Commission adopted a proposal for a Regulation on administrative cooperation through the Internal Market Information System.[12] The Regulation will provide a comprehensive legal framework for IMI, with the following key elements:

- a set of common rules to ensure that IMI functions efficiently, including a clarification of the roles of the different actors involved in IMI;
- a framework for the processing of personal data in IMI;
- a list of legal provisions supported by IMI;
- a possibility of flexible expansion of the system to other policy areas.

For updates on the legislative procedure and the final text, please refer to the IMI website:

❯ **http://ec.europa.eu/imi-net**

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 1995/281, p. 31, as amended by Regulation (EC) No 1882/2003, OJ L 2003/284, p. 1; Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ 2001/8, p.1.

[12] COM(2011) 522 final.

European Commission

The Internal Market Information (IMI) System — User handbook — Update 2012

Luxembourg: Publications Office of the European Union

2012 — 57 pp. — 21 x 29.7 cm

ISBN 978-92-79-26040-7
doi: 10.2780/75733

KM-30-12-755-EN-N

ISBN 978-92-79-26040-7

9 789279 260407

doi:10.2780/75733

Publications Office