EUROPEAN COMMISSION
Internal Market and Services DG

Services
Administrative cooperation and Member State networks

ADMINISTRATIVE COOPERATION UNDER THE SERVICES DIRECTIVE

THE ALERT MECHANISM AND THE INTERNAL MARKET INFORMATION SYSTEM (IMI)

Guidelines and user manual

Commission européenne, B-1049 Bruxelles / Europese Commissie, B-1049 Brussel - Belgium. Telephone: (32-2) 299 11 11.

http://ec.europa.eu/internal_market/

INTRODUCTION

The Services Directive, in its articles 29(3) and 32(1), requires Member States to inform other Member States and the Commission about any service activities that might cause serious damage to the health or safety of persons or to the environment (**'alert mechanism'**). This information should help Member States prevent risks and protect service recipients.

The rapid and secure exchange of information for the purposes of the alert mechanism is ensured through the use of a specific application of the **Internal Market Information System (IMI).**

This document is intended as a **practical guide** for Member State authorities dealing with alerts in IMI. It consists of two parts:

Part 1: Guidelines on the use of the alert mechanism

The guidelines aim to foster a common understanding of the **criteria and conditions for the sending of alerts**. They should help to ensure that alerts are sent only when this is strictly necessary and when the criteria set out in the Services Directive are met. The guidelines also explain when to use the various other functions of the IMI system for alerts, such as the closure, withdrawal and rectification of alerts. Several examples illustrate circumstances in which the functions may need to be used in practice.

Part 2: IMI user manual for alerts

The user manual deals with the **technical aspects** of handling alerts in IMI. It identifies the different roles that authorities and individual users can play in relation to the alert mechanism and it describes how to use all the functions that are available in IMI for each stage of the alert process. It also explains how to set up the system so that alerts can be dealt with effectively.

For more information on the Services Directive, please visit http://ec.europa.eu/internal_market/services/services-dir/index_en.htm.

More information about the IMI system is available at http://ec.europa.eu/internal_market/imi-net.

If you have a technical problem related to alerts in IMI, please contact the IMI coordinator who registered you in IMI. For technical problems that cannot be resolved locally, the Commission has set up a helpdesk that can be reached at: ec-imi-alerts@ec.europa.eu.

TABLE OF CONTENTS

PART 1: GUIDELINES ON THE USE OF THE ALERT MECHANISM

1. INTRODUCTION: WHAT ARE THE GUIDELINES FOR?

The Services Directive, in its articles 29 (3) and 32 (1), requires Member States to inform other Member States and the Commission about any service activities that might cause serious damage to the health or safety of people or to the environment ('alert mechanism'). This information should help Member States to prevent risks and protect service recipients.

The rapid and secure exchange of information under the 'alert mechanism' will be ensured through the use of a specific application of the Internal Market Information system (hereafter 'IMI').

It is also important to have a common understanding of the criteria and conditions for alerts, to reduce the risk of unnecessary or unfounded alerts being sent. In addition, a common understanding is needed on the use of the additional various other functions in the IMI system, e.g. the closure, withdrawal/cancellation and rectification of alerts and the sending of additional information.

The present guidelines are based on the concepts used in the Services Directive and in no way narrow down or extend the obligations on Member States. They are designed to help Member States to give guidance to the national authorities dealing with the alert mechanism.

The Guidelines are not exhaustive and make no attempt to take account of all possible situations and circumstances. National authorities should judge each case on its merits, taking into account the criteria set out in the Services Directive, their own experience and practice, and any other relevant considerations and methods.

It is important to note that the Guidelines are without prejudice to national rules on who is responsible for sending an alert or adopting measures.

Given the impact that an alert may have on the service provider, Member States will need to ensure that the subject of an alert enjoys adequate protection at all times (before, during and after the sending of alerts). It is particularly important to ensure that alerts are only sent when this is really justified. The Guidelines are limited to the substantive criteria for an alert to be sent, closed, withdrawn and rectified, and for the sending of additional information. They do not deal with the application of Community or national rules on rights of defence.

TABLE 1: CHECKLIST: ASSESSING WHETHER TO SEND AN ALERT

Step 1	Is the serious potential danger related to a service activity / to the conduct of a service provider?	→ No × → No alert					
Step 2	↓ Yes √→	Is the service activity covered by the Services Directive?	→ No × → No alert				
Step 3	↓ Yes √→	↓ Yes √→	Is there a danger of serious damage to the health or safety of people or the environment?	→No × → No alert			
Step 4	Yes√	Yes √	↓ Yes √→	Is there a causal link between the service provision and the potential serious damage?	→No × → No alert		
Step 5	Yes√	Yes√	Yes √→	↓ Yes √→	Is there an actual/concrete risk of the serious damage happening?	→No × → No alert	
Step 6	Yes√	Yes√	Yes√	Yes√	↓ Yes √→	Is there a risk of the damage occurring in other Member States?	→ No × → No alert
All steps completed?... Yes √→	SEND ALERT						

TABLE 2: 'TRADE-OFF': SERIOUSNESS OF DAMAGE – LIKELIHOOD OF DAMAGE OCCURRING

	(Probability smaller←) Probability (→ Probability higher)	
(More serious potential damage)←Serious potential damage →(Less serious potential damage)	Case 4: less serious potential damage and relatively low probability of it occurring **In general do not send out alert**	Case 3: less serious potential damage and relatively high/very high probability of it occurring **Send out alert in some cases**
	Case 2: (very) serious potential damage and relatively low probability of it occurring **In general send out an alert**	Case 1: (very) serious potential damage and relatively high/very high probability of it occurring **Send out alert**

Note: the aim of this table is to illustrate the possible trade-off between the seriousness of the potential damage and the likelihood of it occurring. It does not take into account the other criteria for sending alerts described in these Guidelines, which also have to be met before an alert can be sent.

TABLE 3: STEP BY STEP ASSESSMENT OF WHEN TO SEND AN ALERT

Step 1: Is the serious potential danger related to a service activity / to the conduct of a service provider?

☐ Yes, the serious potential danger is related to a service activity / to the conduct of a service provider.

→ go to step two

☐ No

→ do not send the alert

Step 2: Is the service activity covered by the Services Directive?

If you are not sure, click here for more information:

http://ec.europa.eu/internal_market/services/docs/services-dir/guides/handbook_en.pdf

☐ Yes

→ go to step three

☐ No

→ do not send the alert

Step 3: Is there a danger of serious damage to the health or safety of people or to the environment?

When assessing this, consider the gravity and extent of the potential damage. When the gravity is particularly high or the extent is particularly large, an alert may have to be sent even when the probability of damage occurring is low.

☐ Yes – the conduct, specific acts or circumstances relating can cause serious damage to the health or safety of people or the environment

→ go to step four

☐ No, there is insufficient danger of serious damage

→ do not send the alert

Step 4: Is there a causal link between the services-related situation and the potential serious damage?

☐ Yes, there is a causal link. The potential damage would be due essentially to the conduct, specific acts or circumstances.

→ go to step five

☐ No – no direct causal link between the conduct, specific acts or circumstances and the potential serious damage could be established

→ do not send the alert

Step 5: Is there an actual/concrete risk of serious damage? When assessing this, take into account the following elements in particular:

- Does the risk of serious damage still exist or is it likely to occur in the near future? *(if not, do not send the alert)*
- Has anything been done to eliminate or reduce the risk? *(if this action has eliminated the risk/ if the residual risk is insignificant, do not send an alert)*
- Who is the average type of recipient of the service? *(if the recipient is the kind of person who finds it harder to identify the risk or take precautions, the risk of damage is generally higher)*

☐ Yes, there is a real risk of serious damage.

→ go to step six

☐ No, the risk does not persist/ is not likely to recur in the near future.

→ do not send the alert

Step 6: Is there a risk of the damage occurring in other Member States?

When assessing this, consider the following elements in particular:

- Is the provider providing services in other Member States?
- Is the provider established in a border region?
- Is the type of service likely to be provided across borders?

☐ Yes, there is a cross-border effect.

→ send the alert

☐ No, there is no cross-border effect.

→ do not send the alert

2. OVERVIEW OF THE CRITERIA FOR SENDING AN ALERT

The requirements for sending an alert and the related criteria are set out in Articles 29(3) and 32(1) of the Services Directive. Article 29(3) covers cases where the Member State of establishment gains knowledge of conduct or acts that could create a serious danger, whereas Article 32(1) contains a similar information obligation for Member States other than the State of establishment. While both articles address different situations, they serve the same purpose and are based on essentially similar principles and criteria. The criteria for sending alerts are therefore as follows:

a) the conduct, specific acts or circumstances relate to a service activity;

b) there is danger of serious damage to the health or safety of people or to the environment;

c) there is a causal link between the services-related situation and the potential serious damage;

d) there is an actual risk;

e) the risk has a cross-border effect.

For an alert to be sent, **all** of these criteria have to be met in the specific situation at hand.

3. THE CRITERIA IN DETAIL

3.1. CONDUCT, SPECIFIC ACTS OR CIRCUMSTANCES RELATING TO A SERVICE ACTIVITY

3.1.1. Situations covered

An alert should only be sent when it has been established that serious damage could be caused by a service activity **which falls within the scope of the Services Directive**[1]. For instance, the 'alert mechanism' does not cover situations where the risk of damage is created by transport services, health services or private security services, as these are excluded from the scope of the Services Directive.

The fact that a service is provided lawfully in a Member State does not mean that Member State cannot send an alert for conduct or specific acts that, in the context of the provision of that service, create a risk of serious damage to the health or safety of people or to the environment.

[1] Article 2 of the Services Directive. For further explanations on the scope of the Services Directive, see Section 2.1 of the Handbook on the Implementation of the Services Directive at http://ec.europa.eu/internal_market/services/docs/services-dir/guides/handbook_en.pdf.

The risk of serious damage should arise in the **conduct** of the service provider or in any **other circumstance** relating to a service activity. Thus, an alert should not be sent for any conduct or action which might result in danger but which **is not related to the provision of services**.

Example

If a service provider who provides language courses is arrested for dangerous driving, there will be no reason to send an alert to other Member States. The conduct posing the danger has no connection *with the provision of the service.*

Examples of conduct that may create risks are[2]:

- **Positive action** by the service provider, such as dangerous conduct or the provision of false information (e.g. irresponsible treatment of waste which could harm the environment, or the provision of faulty nutritional advice which could harm people's health).
- **Lack of action or supervision** by the service provider, such as the failure to adopt necessary preventive measures or the lack of essential instructions to service recipients (e.g. on the maximum duration of a session in a solarium).
- The **inappropriate use of safe equipment or the use of dangerous equipment** for the provision of the service (e.g. the indoor use of sound equipment that is meant for outdoor use only, or the use of unsafe attractions at travelling fairs).

3.1.2. Situations in which the alert mechanism cannot be used — linkage between the Services Directive alert mechanism and existing product alert mechanisms

For this alert mechanism, **the risk must relate to conduct, specific acts or circumstances within the context of a service activity**.

The alert mechanism should not be used in cases where the risk originates in consumer products. In those cases, the rapid alert systems for products should be used[3]. This will give Member States details of the danger of the product so that they can take steps to have it withdrawn from the market.

However, in certain cases, **the conduct of the service provider may be linked to the use of products as part of a service provision** and, if there is a serious risk, the alert mechanism will need to be used. This would be the case, for instance, if a service provider made **inappropriate use of safe products** in providing a service, resulting in a risk to the health or safety of persons or to the environment.

Example

For certain beauty treatments, service provider X uses anaesthetic creams at a dosage above that indicated. The inappropriate use of these creams causes a risk

[2] When deciding whether to send an alert, there is no need to establish fault or negligence in relation to the conduct in question.

[3] i.e. the rapid alert systems for non-food consumer products (RAPEX), food and feed (RASFF) or medicinal products – 'vigilance' system for medical devices.

to people's health. As the misuse of an anaesthetic (not the anaesthetic as such) renders the service unsafe, the Services Directive alert mechanism should be used.

Another scenario is when a dangerous product is used in the provision of a service. This may require a complementary alert to be sent through the Services Directive alert mechanism even if an alert has already been sent through an alert mechanism for products. This would be the case, for example, if a service provider continued to use dangerous consumer products in the provision of a service activity, despite those products having been withdrawn from the market or recalled by producers or distributors.

Example

A RAPEX alert reports a dangerous toy, which is subsequently withdrawn from the market in all Member States. Member State A is aware of the fact that children's entertainer X is continuing to use the dangerous toy in his performances in several Member States. This conduct could do serious damage to the health of the children. Member State A should send an alert through the Services Directive alert mechanism notifying the danger of the entertainment service provided by X.

3.2. SERIOUS DAMAGE TO THE HEALTH OR SAFETY OF PEOPLE OR TO THE ENVIRONMENT

For an alert to be sent, the potential damage to the health or safety or people or to the environment must be **serious**. Two factors that seem particularly relevant here are: (a) the potential gravity of the damage, and (b) the potential extent of the damage.

3.2.1. Gravity of the damage

Assessing the potential gravity of the damage should be based on considering the possible consequences of the conduct of the service provider or of the circumstances.

- **Serious damage to the health or safety of persons** would include damage to their physical or mental integrity, such as serious injuries (e.g. fractures, damage to internal organs, damage to sight or hearing, severe skin burns or cuts, etc.), chronic or other serious diseases, mental disorders, etc.
- **Serious damage to the environment** (natural and urban) would include serious pollution in its diverse forms (air and water pollution, soil contamination by herbicides, pesticides or heavy metals, noise and light pollution), fire damage and the destruction of ecosystems and biodiversity.

3.2.2. Extent of the damage

The number of people or the area that might be affected should be taken into account when estimating the seriousness of the potential damage. When the extent is particularly large, the seriousness of the damage will logically be higher.

Example

A service provider established in Member State A fails to comply with hygienic standards, and its provision of catering services has caused mild food poisoning in a large number of persons in Member State B. Although in principle mild food poisoning could be regarded as a non-serious damage to people's health, the large number of people potentially affected means that the damage can still be considered serious.

3.3. CAUSAL LINK BETWEEN THE SERVICES-RELATED SITUATION AND THE POTENTIAL SERIOUS DAMAGE

There must be a **direct causal link** between the conduct or circumstances and the potential serious damage.

This will not be present when the risk of damage engendering an alert has been provoked or caused to a very substantial degree by *force majeure* or a third party (including the service recipient).

Example

Service recipient X suffers serious damage due to failure to comply with the instructions he was clearly requested to follow when using diving equipment. In this case, the damage does not originate in the conduct of the service provider but rather in the conduct of the service recipient.

3.4. ACTUAL/CONCRETE RISK

It is important to note that knowledge of dangerous conduct or specific acts on the part of a service provider in a Member State should not automatically result in that Member State sending an alert. The important thing is to estimate the **actual existence of a risk**. There will be actual risk when a dangerous situation relating to a service activity:

- **still exists** at the time the alert is sent or
- is (sufficiently) **likely to occur** in the (near) future.

Whether there is **sufficient likelihood** of a dangerous situation arising in the future is something that has to be determined considering all the **facts/circumstances**, in particular whether such dangerous situations or possible damage have occurred in the past and whether there are indications that there may be changes in the conduct of the provider or in the circumstances.

Purely fortuitous accidents are neither predictable nor preventable. If there is no evidence that an accident which occurred during the course of the provision of a service might happen again, there will be no need to send an alert, no matter how serious the resultant damage may be.

Example

Service provider X provides an innovative skin treatment that poses a clear danger to the health of persons. There are grounds for believing that there will be no change in the conduct of service provider X unless such change is enforced. The risk of damage will continue as long as service provider X continues providing services. Any Member States that become aware of the damage should alert the Member State of establishment and any Member States in which X may be expected to provide services.

Certain services entail an **inherent degree of risk**, such as certain 'high risk' sports (e.g. paragliding, parachuting, bungee-jumping, etc.) or such events as urban car rallies.

When an intrinsically dangerous service is carried out lawfully in a given Member State, it is clear that no alert should be sent to any other Member States. However, if any conduct or specific acts of a given service provider were to substantially increase the risk inherent to such a service, an alert should be sent informing other Member States of the danger posed by the conduct or specific acts of the service provider in question (provided that all the criteria necessary for sending an alert are met).

Example

If Member State A allows the provision of bungee-jumping services, it cannot send an alert if it finds that that service provider X is lawfully providing such services in its territory. However, if there is evidence that service provider X is increasing the risk which is inherent to bungee-jumping by providing services which do not comply with safety requirements, Member State A should then send an alert to the Member State of establishment of X.

Clearly, if the potential damage is particularly serious even a low probability of the damage happening in the future may justify the sending of an alert.

Two factors seem to be of particular importance here: (a) the effect of any measures adopted by the service provider or by Member States with a view to eliminating or reducing risk, and (b) the average type of recipient of the service and their capacity to apprehend and avoid the risk.

3.4.1. Effect of any measures adopted by the service provider or by a Member State with a view to eliminating or reducing risk

Under certain conditions, measures adopted voluntarily by the service provider might eliminate the risk. Likewise, measures adopted by the Member State of establishment or by other Member States in conformity with EC law and, in particular, with the Services Directive, can considerably reduce the risk or eliminate it entirely. In the absence of risk, no alert should be sent.

In general, the Member State of establishment will be able to take steps to eliminate the risk, so it follows that more alerts will be sent by Member States other than the country of establishment.

3.4.2. Type of recipient and their capacity to apprehend and avoid the risk

In assessing the likelihood of a danger, it is also important to take into account **the average service recipient's knowledge of the risk and the possibility of taking precautions against it** so that the risk can be graded.

The knowledge of the risk may depend on the **type of user of the service**. When a service is provided from business to business, the recipients may be more aware and better able to take precautions than when a service is provided from a business to an individual consumer. Similarly, when a service is for the elderly, children or the physically or mentally disabled, the risk of damage resulting from a conduct or specific act might be higher.

Example

A Member State becomes aware of a service activity which involves children and could cause serious damage to their safety. Since children are generally less aware of the risk and are therefore unable to take precautions against it, the likelihood of the damage occurring seems to be higher than where the risky activity targets adults.

For other groups of persons, the likelihood of damage might be higher where the service provider does not provide adequate safeguards, warnings or instructions, and the hazard is not obvious.

Example

Service provider A provides nutritional advice which can cause considerable damage to persons suffering from specific nutritional imbalances. Recipients seem to be unaware of this danger. Given the novelty of the nutritional advice, there is very limited information on the risks among the public in general. When assessing whether damage is likely to happen in the future, Member States need to bear in mind that adults will not be able to take sufficient precautions against it.

3.5. NEED FOR RISK TO HAVE A CROSS-BORDER EFFECT

Before a Member State sends an alert, it should ascertain that there is sufficient likelihood of the damage occurring **in other Member States,** which means considering any factors that might indicate that the service provider is likely to be active in other Member States.

Obviously, the risk of damage occurring in another Member State may be more readily assumed if the service provider is established in a Member State other than where the risk arises. Indications may also be derived from the type of service or the location of the place of establishment of the service provider, which (if geographically close to another Member State) might suggest activity in other Member States. For online services, the existence of a cross-border effect may be more readily assumed.

When the damage is caused by the use of defective equipment which may be used in other Member States, it will be easier to establish the cross-border effect of the risk.

4. WHO SENDS AN ALERT?

The Services Directive distinguishes between alerts sent by the Member State of establishment (Article 29(3)) and others (Article 32(1)). These two situations are examined separately below.

4.1. ALERTS SENT BY THE MEMBER STATE OF ESTABLISHMENT

In many cases, the Member State of establishment will not need to issue an alert because, as soon as it becomes aware of a serious danger to the health or safety of persons or to the environment, it will generally take immediate measures to prevent any risk. These should, in general, ensure that the risk ceases to exist (e.g. a service provider is no longer authorised to carry out his activities, defective equipment has been repaired, etc.). In the absence of a (persisting) risk of serious damage to the health and safety of persons or to the environment in other Member States, no alert should be sent.

However, there are instances in which the Member State of establishment may need to send an alert despite measures having been taken, for example:

- When the Member State of establishment is not certain that the measures taken against the service provider can be effectively enforced or are sufficient to stop the risk from arising.

  Example

  Member State A receives complaints about a service provider who is creating a very serious risk to the health of service recipients. Immediate and effective measures to eliminate or prevent the risk cannot be adopted at the place of establishment because the service provider is currently outside its territory providing services in other Member States.

- When the Member State of establishment is aware that the service provider is using the same equipment to provide services in other Member States.

  Example

  Member State A is aware that service provider X organises bicycle tours in A and in Member State B. In Member State A, X is using bicycles which are not properly maintained, thereby creating a risk to the safety of persons. Member State A has strong reason to believe that the same bicycles are being used in Member State B.

- There may be occasions where the serious damage to the health and safety of persons will not follow on immediately from the conduct or specific acts which cause it, but will only be revealed at a later stage. Where the

conduct or specific acts that create the risk have already taken place in other Member States, it will no longer be possible for the Member State of establishment to do anything to eliminate the risk. In these cases, an alert should be sent so that other Member States can take their own steps.

Example

Service provider X, established in Member State A, is in the ceiling business. Some of his ceilings collapsed, causing serious risk of damage to the people in the apartments. Inspections revealed that the collapse was due to negligence. Member State A is aware that provider X has worked in other Member States and therefore sends an alert to all Member States to help prevent further damage.

The fact that measures have not been adopted by the Member State of establishment does not prevent that Member State from sending an alert. However, if the non-adoption of measures is due to a lack of evidence on the existence of risk or on the seriousness of potential damages, that Member State should not send an alert to other Member States.

Example

Member State A receives several complaints against service provider X, accusing X of causing serious risk to people's health. The complaints are manifestly unfounded. As a result, no measures are adopted against X. In this event, Member State A should not send an alert to any other Member States.

4.2. ALERTS SENT BY MEMBER STATES OTHER THAN THE STATE OF ESTABLISHMENT

When a Member State other than the country of establishment becomes aware of serious specific acts or circumstances that could cause serious damage to the health or safety of people or to the environment in its territory or in other Member States, that Member State must inform the Member State of establishment, the other Member States concerned and the Commission as quickly as possible.

In most cases this type of alert is likely to be sent by the Member State where the service is provided.

Unlike measures taken by the Member State of establishment, measures taken by the country where the service is provided will often only prevent risks in its own territory. As a result, risks for other Member States may remain. In such cases, an alert would still need to be sent to the Member State of establishment, any other Member State(s) concerned and the Commission.

Example

Service provider X, established in Member State A, is providing industrial cleaning services in Member State B. Following complaints, Member State B carries out an inspection and finds out that X has disposed of waste generated during his work in a dangerous manner that causes risk of serious damage to the environment. The authorities of Member State B have indications that X is

continuing this practice. X is also offering his services in Member States C and D. As a precaution, they send an alert to the Member State of establishment A, Member State C and Member State D.

Upon receipt of such an alert, the Member State of establishment should examine the case and take measures to prevent the risk in general.

4.3. ALERTS SENT BY THE MEMBER STATE OF ESTABLISHMENT LINKED TO A PREVIOUS ALERT BY ANOTHER MEMBER STATE

Where, despite measures taken by the Member State of establishment, the risk persists, the Member State of establishment will, on the strength of Article 29(3) of the Services Directive, need to inform all other Member States concerned, i.e. an alert will be sent to those Member States which have not yet received the alert, and updated information will be transmitted to the other Member States[4].

5. WHO SHOULD RECEIVE AN ALERT?

The Services Directive distinguishes between alerts sent by the Member State of establishment (Article 29(3)) and others (Article 32(1)). When Member States need to determine which Member States are concerned by an alert, competent authorities may take into account the following factors:

- records of provision of services in other Member States in the past. This factor will become even more relevant if the provision of services in another Member State is conducted by the same person whose conduct is causing the danger, or using the same equipment as is creating the risk.
- the type of service.
- the place of establishment of the service provider.

6. THE CLOSURE OF ALERTS

6.1. WHEN SHOULD AN ALERT BE CLOSED?

To protect service providers who are the subject of alerts, alerts must be sent out only when justified, i.e. when all the criteria described in Section III of these Guidelines are met. It is equally important to ensure that alerts are closed as soon as the underlying cause ceases to exist.

Usually the closure of the alert will be prompted by the disappearance of the risk of serious damage to the health or safety of persons or to the environment. For example, the service provider may have taken voluntary measures to eliminate the risk (e.g. has replaced defective equipment or has provided proper instructions to recipients, thereby putting an end to the risk which gave rise to the alert). It could also be that the risk has disappeared because of steps taken by Member States, in conformity with Community

[4] To avoid confusion and for the sake of consistency, this new information will be clearly linked to the existing alert in the system.

law (e.g. the Member State of establishment may have temporarily suspended the provider's authorisation to exercise his activities).

The knowledge that the risk no longer exists can be self-acquired by the Member State of establishment and/or might result from information transmitted by other Member States through the alert mechanism (See Section IX below). Once the risk is known to have disappeared, the Member State which sent the alert should immediately send a proposal to close it.

6.2. OBJECTING TO CLOSURE

To prevent misuse of the closure function and to avoid situations in which an alert is closed despite one or more Member States knowing that the risk persists, the proposal for closure will need to be duly motivated and the other Member States involved should be able to object to closure if they have evidence that the risk persists. The Member States involved in an alert should be able to object to closure only if they have specific indications that the risk still persists. Member States should therefore provide reasons and substantiate their possible objections.

7. WITHDRAWAL/CANCELLATION OF ALERTS

The criteria for sending alerts outlined in these Guidelines are designed to prevent unjustified or unfounded alerts being sent. Despite these safeguards a Member State may still send an alert on the strength of information or evidence which was wrongful or inaccurate, but where the error is discovered only at a later stage.

Example

The competent authorities of Member State A have indications that service provider X, who is established in Member State B and is providing construction services in Member State A, has unlawfully disposed of waste in its territory, thereby creating environmental damage. Member State A sends an alert to Member State B to prevent further damage. Further checks carried out by Member State A point to the waste being dumped not by service provider X but by service provider Y, who was working on the same site as provider X. Service provider Y is established in Member State A and does not provide cross-border services. Therefore, Member State A withdraws the alert.

Once the error becomes known, the Member State which sent the alert should immediately send a request to withdraw/cancel it. This will automatically be communicated to all recipients of the original alert. An explanation should be given of why the alert was unfounded (and therefore needs to be withdrawn).

It is important to note that an alert should only be withdrawn where the Member State which initiated it realises that the criteria for sending the alert were not valid in the first place. If the risk existed at the time the alert was sent but subsequently disappeared, the alert should be closed (and not withdrawn), as described above.

8. RECTIFYING INFORMATION

However carefully alerts are checked and substantiated before sending, they may still need to be rectified at a later stage. This may happen, for instance, if the initial information contained in the alert turns out to be partially wrong. For example, at the time of the sending of the alert the initiating Member State may have entered the wrong name or address of the service provider (or may not have provided this information at all because it did not have it). In these cases, it is important that the initial alert be rectified as soon as the faulty information comes to light.

9. SENDING ADDITIONAL INFORMATION

With a view to minimising risk and ensuring good cooperation between Member States, it is important for the information contained in an alert to be as complete as possible and that Member States involved in an alert have all relevant information at their disposal. It will be important in particular to supply additional information if this can help speed up the closure of the alert or boost other Member States' awareness of the existence of a serious risk. This will give the Member State which sent the alert and all other Member States involved the chance to provide the other Member States with feedback or additional information on alerts, which will be clearly linked to the original alert message. Examples of this are where:

- the Member States which have received the alert want to confirm that the service concerned is indeed being provided in their territory and that they either confirm or refute the information contained in the initial alert on the basis of their observations/indications;
- the Member States which have sent or received the alert want to provide information on measures they have taken against the service provider, in conformity with Community law, to reduce or eliminate the risk;
- the Member States which have received the alert want to request additional information from the Member State which sent the alert, for instance if the information contained in the alert was held to be unclear or incomplete;
- the Member States which have received the alert want to tell the other Member States that, from their perspective, an alert could be closed because in their view the risk no longer persists (in their territory).

It is important to avoid sending repetitive or irrelevant/unimportant information on alerts.

PART 2: IMI USER MANUAL FOR ALERTS

10. INTRODUCTION

This user manual deals with the **technical handling** of alerts in the Internal Market Information System (IMI). It identifies the different roles that authorities and individual users can play in relation to the alert mechanism and it describes how to use the functionalities that are available in IMI for each stage of the alert process. It also explains how to set the system up so that alerts can be dealt with effectively in each country.

The manual focuses on those functions of IMI that are **immediately related to alerts**. For general information about using IMI, e.g. how to register and log in, and about handling the standard information exchange in IMI, please refer to the material available on the IMI website (http://ec.europa.eu/internal_market/imi-net/training_en.html), especially:

- The **IMI User Handbook**; and
- The **interactive learning modules** ('Captivates').

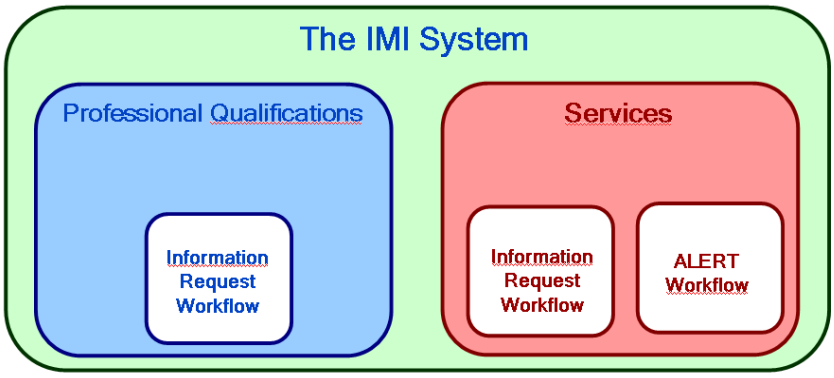
For guidance on the criteria and conditions for sending alerts, please refer to the first part of this document, the "guidelines on the use of the alert mechanism".

11. ALERTS IN THE IMI SYSTEM

11.1. The modular structure of IMI

IMI is a single information system made up of individual building blocks (**modules**) for each legislative area in which it is used. A module supports one or more processes (**workflows**). In the IMI module for the Services Directive, there is one workflow for the standard information exchange and a separate workflow for the alert mechanism. Access to each workflow is restricted to authorities who are specifically registered for it. This means that an authority whose task it is to deal with alerts in IMI needs to have access to (1) the IMI system, (2) the services module and (3) the alert workflow.

Legislative areas and workflows in IMI



11.2. The alert lifecycle

The basic lifecycle of an alert consists of five steps, which are determined by their actors.

(1) Any authority registered for the alert workflow in any Member State of the European Economic Area (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 coordinator in its own Member State. The alert coordinator **checks** the alert and **broadcasts** it to other Member States.

(2) In each recipient Member State, an alert coordinator that has been 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 **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. In a case where 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 agreement has been reached amongst them, a selected alert coordinator (the **"closing coordinator"**) can **broadcast the closure proposal** to all other Member States concerned.

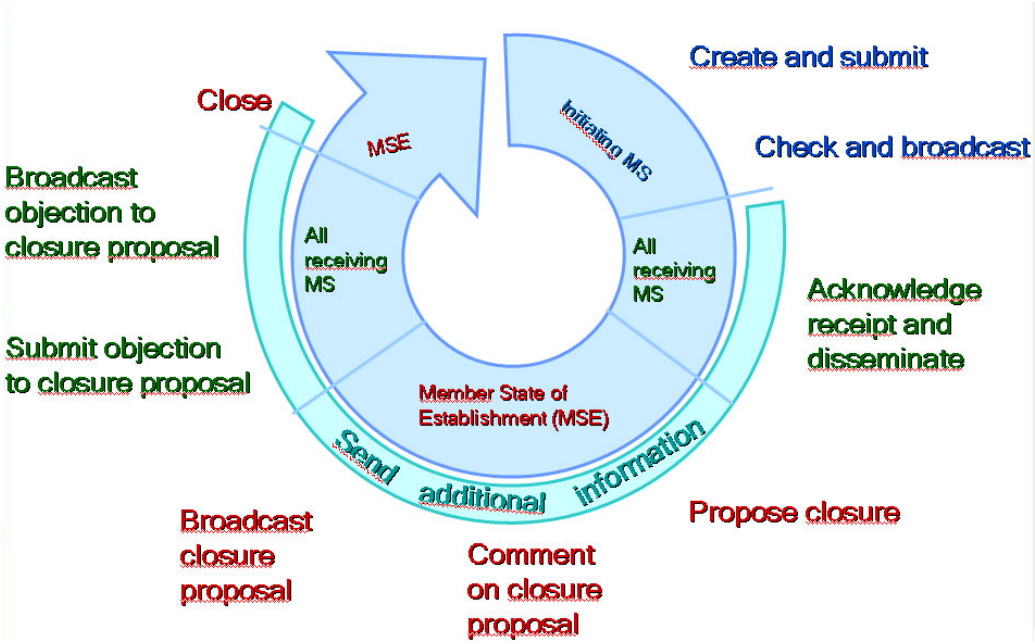
(4) Subsequently, all other Member States that received the alert have the possibility to **object to its closure** if they have information that the risk persists. Alert authorities **submit** such objections to an alert coordinator, who can **broadcast** them to all other Member States involved.

> 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, it is possible at any time and for all Member States involved to add further information to the alert.

Overview of the alert lifecycle



12. ALERT ACTORS AND THEIR ROLES

12.1. 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**. One alert coordinator will be designated as the **incoming alert postbox** for its Member State.[5] These roles are independent from the roles that the authority concerned may play in IMI in other respects. 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.

12.1.1. 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. In case another Member State proposes closure, they can **submit objections** to the closure of the alert to their alert coordinator.

---

[5] 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.

12.1.2. Alert coordinator

The task of alert coordinators is to ensure that alerts are only broadcast when this is necessary and that they are treated adequately. In general, they will have competences in the field of health and safety of persons or in the field of 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**, **broadcast proposals to close** an alert and, in case another Member State proposes closure, **broadcast objections to closure**. In addition, 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.

12.1.3. Alert coordinator flagged as incoming alert postbox

An alert coordinator that is nominated as the incoming alert postbox is the central entry point for alerts in its Member State. It **acknowledges receipt** of an incoming alert and is responsible for a **first 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 that the incoming alert postbox has a good knowledge of the administrative structures of its Member State.

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

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

12.1.4. 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 possibility to **edit or delete the content** of alerts or alert-related information submitted to them. If it is decided that an alert coordinator should have this possibility, a tick-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.

Where a coordinator does not have final approval, the initiating authority retains the right to edit or delete the alert or alert-related information that it submitted.

12.2. 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.[6] He can then assign different user roles to his colleagues according to the size of the authority and their responsibilities concerning alerts.

12.2.1. 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.

12.2.2. Alert handler

The task of "alert handlers" is to 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 **submit and request additional information** relating to an alert. They can submit a closure proposal, they can comment on closure proposals submitted by other authorities in their own Member State and they can submit objections to closure if another Member State proposed closure. However, alert handlers in an alert coordinator **cannot broadcast or disseminate** alerts.

12.2.3. Alert disseminator (only for alert coordinators)

The user role "alert disseminator" is only available to users in an alert coordinator. Alert disseminators are responsible for the **dissemination** of 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 a first 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 in their field of competence should receive the alert.

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

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. With this setting, alert disseminators can also **delete** the alert or alert-related information prior to broadcast.

12.2.4. Basic user

All IMI users in an authority with access to the alerts workflow who are not local data administrators and who are not assigned any of the specific workflow roles described above, automatically receive a basic access to alerts. They have a **high-level overview** of all alerts (incoming and outgoing) of their authority, but are not able to see the details of the alerts. They are **not able** to initiate alerts or to **take any action** on ongoing alerts.

---

[6] In case there are several users with local data administrator rights, all of them are given all user rights for alerts.

This is also the default access for everybody in the authority who already uses the information request workflow in the IMI services module. Thus, for example, a request handler is automatically given basic user rights for alerts. If he needs to play a more active role in relation to alerts, this role can be assigned to him in addition to his request handler role.

12.2.5. Combined roles

IMI also 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**.

However, it should be borne in mind that submission and broadcast remain **separate steps**, which need to be completed individually, even if this is done 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)*
Initiating an alert	Submit	√	
	Broadcast		√
Sending/requesting additional information	Submit	√	√
	Broadcast		√
Withdrawing an alert *(initiating authority and coordinator only)*	Submit	√	
	Broadcast		√
Proposing closure of an alert *(in MSE only)*	Submit	√	
	Comment	√	√
	Broadcast		√
Objecting to a closure proposal	Submit	√	√
	Broadcast		√
Closing an alert *(coordinator that broadcast closure proposal only)*			√

13. HANDLING ALERTS IN IMI

Alerts have a clearly defined **lifecycle** consisting of a number of basic steps (see section 2.2) and additional optional steps that may not need to be used in every case. As the alert moves from one step to the next, its **status** is automatically updated and displayed on the screen.

13.1. Sending an alert

13.1.1. Initiate and submit an alert

In order to be able 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 Part 1 of this document). IMI automatically leads him through this process. If all criteria are fulfilled, he enters the **data of the service provider** who is causing the potential danger as well as 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 of the data input, 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"

13.1.2. Broadcast an alert

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

If they consider that their authority is not competent to decide on whether or not 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 are indeed 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 modify the alert. If he concludes that the alert should not be sent at all, he can ask the authority to delete it.

Independent of the "final approval" setting, the alert disseminator can always **add recipient Member States** to the alert if, to his knowledge, this 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 foreseen by the Services Directive.

The alert receives the status: **"Alert is Broadcast"**

13.2. Editing and rectifying an alert

After an alert has been broadcast, only the initiating Member State can edit or rectify 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[7],
- change the **service provider details** and
- modify 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 modify 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 about this fact in an automatic email.

13.3. Withdrawing an alert

Despite the built-in safeguards, a Member State may still have sent an alert on the basis of information or evidence which was wrongful or inaccurate, and may discover the error only at a later stage. If it becomes clear that 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**

---

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

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"**.

13.4. Managing recipients of an alert

13.4.1. Acknowledge receipt of an alert

Alerts that were broadcast arrive in the incoming alert postbox of each Member State that was selected as a recipient and at the European Commission.[8]

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 in the status **"Alert Awaiting Acknowledgement"**.

13.4.2. Disseminate an alert

First dissemination of an incoming alert is also the responsibility of alert disseminators in the incoming alert postbox. They select the alert coordinators and alert authorities for whom the alert is relevant and disseminate it to them. 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**.

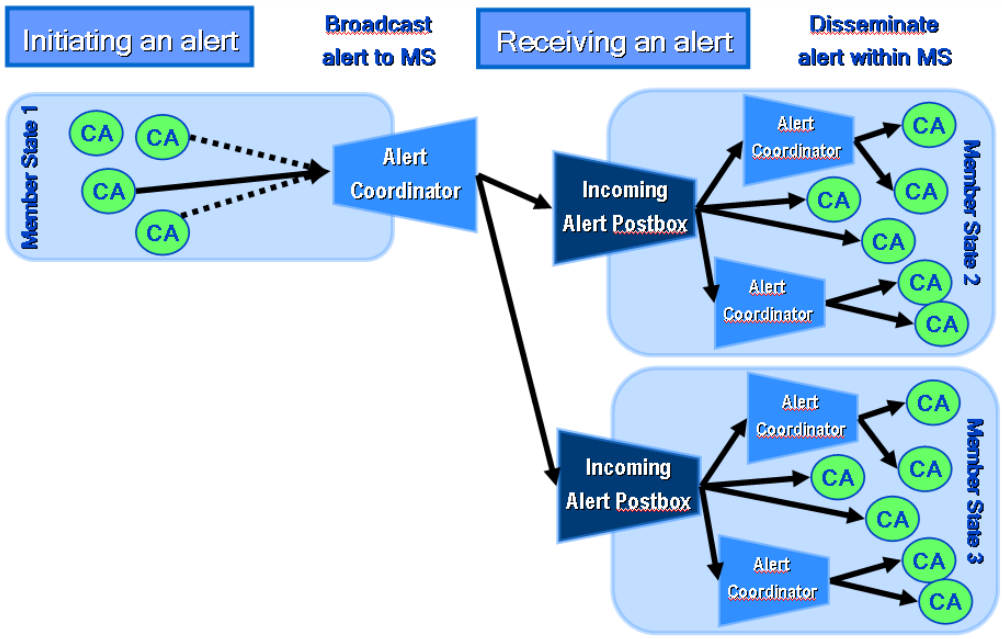
Once an alert has been disseminated, only alert disseminators in incoming alert postboxes can **remove recipients**. Recipients can only be removed if they have not yet taken any action on the alert. This could happen in a case where a recipient finds that an alert is not relevant for his authority and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

---

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



13.5. Sending and requesting 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 (see Part 1 of this document for more examples). If it is not the Member State responsible for closure of the alert, it can also use the additional information function to suggest to that Member State that the alert be closed. Similarly, recipient Member States can **request additional information** from the initiating Member State or from another recipient Member State that contributed information to the alert previously.

Both the sending and the requesting of additional information take place in 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.

13.6. Closing an alert

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

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

The closure process consists of two phases:

- In the first phase, all authorities in the MSE have the possibility to agree on whether closure should be proposed to the other Member States (= **comment period**).

- In the second phase, after the closure proposal has been broadcast, all other Member States involved have the possibility to object to closure if they consider that the alert should remain active (= **objection period**).

13.6.1. Initiate a closure proposal

Alert handlers in any recipient authority in the MSE can **initiate a closure proposal** if they have established 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** (and without any action on the part of 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. However, if the closing coordinator has final approval, it can edit or delete the closure proposal at any time.

> Note that, as the comment phase only involves activity within one Member State, there is no second step to be completed by an alert coordinator at this stage.

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

13.6.2. Comment on a closure proposal

The closure proposal remains **open for comments** within the MSE for a fixed period of time, on which all Member States agreed. 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"**.

13.6.3. 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 via the tab **"Closure Management"**). He can choose to **include individual 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"**.

13.6.4. Object to a closure proposal

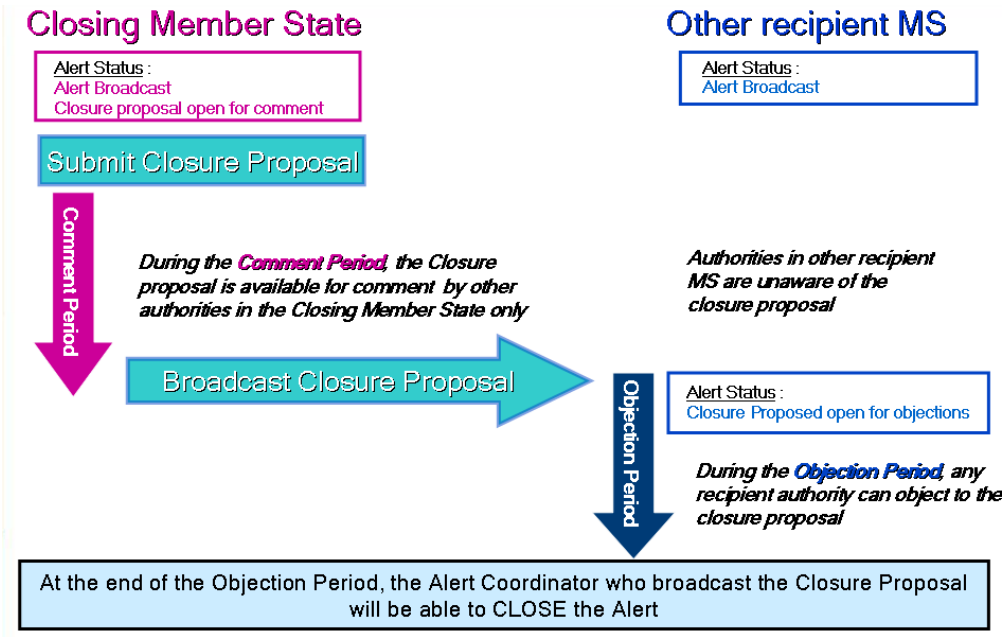
All other Member States now have the possibility to raise any **objections** they may have against the closure of the alert, in case they have information that the risk persists.

The period of time for lodging objections is also determined 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" functionality**, which contains a heading called "Objection to a closure proposal".

The submission and broadcast of objections is a **two-step process** just like the sending of 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 about the objection by automatic email.

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

The comment and objection periods



13.6.5. Close an alert

Taking into account possible objections from 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"**.

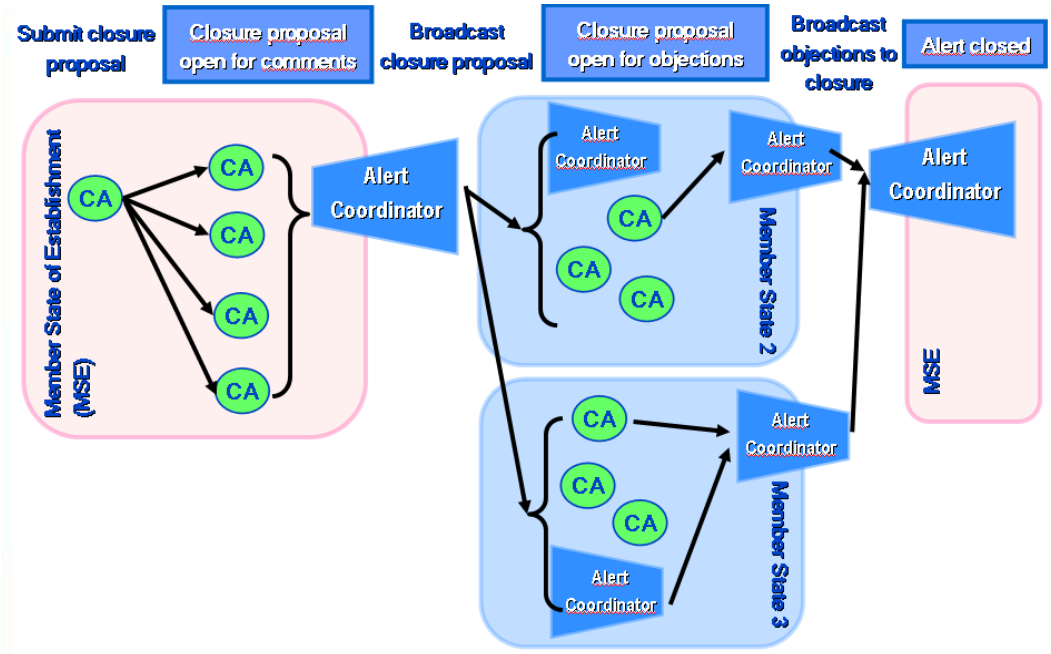
Once the alert has been closed, only limited details remain visible for all users. These include

- 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.

Should a Member State, despite the closure of the alert by the MSE, be convinced that the risk has still not been eliminated, it can **launch a new alert**.

Closing an alert



14. KEEPING TRACK OF ALERTS

14.1. Automatic emails

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

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.

14.2. Alert lists

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

- Alert numbers
- A 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** with a number of different criteria and can also be accessed through the menu option "Search Alerts".

Depending on their user profile, users can open alerts from this list and take action on them.

14.3. 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 the draft status.

Every user is able to print alerts at the level of detail that he is able to see. Thus, basic users can only print the general overview (including the recipient list and history of the alert), whereas alert viewers and alert handlers can print all details contained in an alert.

When an alert has been withdrawn or closed and only the reduced view is still visible, only this reduced view can be printed.

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

15. ALERTS AND DATA PROTECTION

The exchange of information related to alerts in IMI is **necessary to comply with a legal obligation**. It is thus fully lawful from a data protection perspective. However, the Commission is conscious of the data protection implications of such a system. It has therefore taken great care in its design ensuring that it is data protection-friendly and encourages Member States, who are responsible for the application of the data protection legislation when sending or receiving alerts, to **be vigilant** about the correct application of the data protection rules.

The alert mechanism contains a number of **data protection safeguards**:

- **Access** to the data is **limited** to authorities, who are specifically given access to alerts.

- The checklist at the beginning of the process of drafting an alert and the two-step sending procedure involving an alert coordinator make sure that **no unnecessary alerts are sent**.

- The initiating Member State has to assess which other Member State(s) should receive the alert. This and the fact that it is up to the incoming alert postbox to decide which specific authorities should receive the alert in its Member State make sure that alerts are **not distributed more widely than necessary** to comply with the requirements of information.

- As foreseen in the Services Directive, the **Commission** receives all alerts that are being sent. However, it does **not have access to any personal data** contained in the alerts and only sees a reduced view of them.

- In case unfounded alerts have been sent despite all precaution, these can quickly be **withdrawn**. Incorrect data can be **rectified or deleted**.

- Alerts are **closed as soon as the risk no longer persists**. The data immediately becomes invisible to all users, once an alert has been closed, and personal data is deleted 6 months after closure.

For more details on data protection in the context of the alert mechanism and in IMI in general, please refer to the Commission report on the situation of data protection in the Internal Market Information System and the Commission Recommendation on data protection guidelines for IMI[9].

16. ADDITIONAL INFORMATION FOR COORDINATORS - SETTING UP THE NECESSARY STRUCTURES FOR ALERTS IN YOUR COUNTRY

16.1. First registration by the Commission

The only system-related requirement for each Member State to use the alert mechanism in IMI is that it has one authority registered as an **incoming alert postbox**. When the alert mechanism became operational, the Commission registered the **incoming alert postboxes** for all Member States or, in case they were already registered in IMI, granted them access to alerts and assigned them this role.

Registration of further alert coordinators and alert authorities, if required, is the responsibility of the Member States.

By definition, national IMI coordinators (NIMICs) and super-delegated IMI coordinators (SDIMICs) have **full responsibility** in their geographical region for all legislative areas and the associated workflows in IMI. Therefore, the Commission has given all NIMICs and SDIMICs access to the alert workflow. With this access, they are able to **give other authorities in their country access** to the alert workflow.

---

[9] C(2009) 2041final. OJ L 100, 18.4.2009, p. 12.

However, this **administrative role** does not prejudge which **content-related role** NIMICs and SDIMICs play in relation to alerts. They can be assigned any of the authority roles described in section 3.1, depending on their competences and the administrative structure in their country.

16.2. Authority registration and access to the alert workflow

Alert coordinators can be registered and given access to alerts by

- NIMICs
- SDIMICs
- Legislative area coordinators (LIMICs)[10] for the Services Directive

Alert authorities can be registered and given access to alerts by

- NIMICs
- SDIMICs
- LIMICs and
- Delegated IMI coordinators (DIMICs)

In other words, DIMICs cannot register any alert coordinators.

Upon registration of alert coordinators, it is important to determine whether the coordinator in question should have **"final approval"** in the alert workflow (i.e. whether it should be allowed to edit or delete the content of alert-related information submitted to it by an alert authority).

Note that **access to the alert workflow** has to be granted **separately** from **access to the legislative area** of services. Thus, when a new authority is to be registered with access to alerts, it needs to be

1. registered in IMI

2. granted access to the legislative area of services

3. granted access to the alert workflow.

[10] A LIMIC is a role for a coordinator with overall competence for one legislative area. For each Member State there can be only one LIMIC per legislative area.

16.3. Linking authorities and coordinators

When an authority is given access to the alert workflow as an **alert authority**, the authority must be **linked** to at least one **alert coordinator** in its country. Further linked alert coordinators can then be added or deleted subsequently.

It is important that alert authorities are linked to the correct alert coordinators, as they can **only submit alert-related information to an alert coordinator to which they are linked**.

Alert coordinators, on the other hand, can **disseminate alerts to any alert authorities and alert coordinators** in their country, no matter whether they are linked to it or not.