



Agència Catalana de Protecció de Dades

RECOMMENDATION 1/2008

By the Catalan Data Protection Authority on
the transmission by Internet of information
containing personal data



Dr. Esther Mitjans
Director of the Catalan Data
Protection Authority

It is necessary to decide the type of society we want to live in and clarify whether which things that are technologically possible are socially acceptable.

The Catalan Data Protection Authority offers a reminder of the most important principles to be applied in the dissemination of information through the Internet. Based on the Authority's experience, it sets out to provide certain lines of action intended to address the problems detected when data of a personal nature is published through the websites and online centres of public administrations in Catalonia and in Official journals and Gazettes.

This Recommendation does not intend to revolutionise the legal system, but rather to provide an interpretive instrument to those responsible for managing files. This is, in any case, a dynamic tool subject to continuous validation due to constant technological change.

Esther Mitjans Perelló

*Director of the Catalan Data
Protection Authority*

Barcelona, 15 April 2008

Contents

Chapter I. General considerations

1. Object of the Recommendation 3
2. Scope 4
3. Concept of transmission 4
4. Principles 5

Chapter II. Transmission of information by Internet

Section 1a. General conditions for transmission

5. Legitimacy of publication 6
6. Proportionality of the information 7
7. Exactitude and updating of information transmitted 8
8. Time limit on transmission 8
9. Periodic review of web content 9
10. Duty of information 9
11. Exercising the right of *habeas data* 9
12. Security measures 10

Section 2a. Specific conditions

13. Links to other webs 10
14. Web hosting services 11
15. Blogs and discussion forums 11
16. Search tools 11
17. Transmission of personal data regarding infringements, the imposition of penalties and court orders 12
18. Transmission of the minutes of collegial body meetings 13
19. Transmission of personal data in the form of images or voices 14

Chapter III. Publication in electronic official journals and bulletins

20. Search tools 14
21. Duty of information and exercising the right of *habeas data* 15
- Annexes* 17

Recommendation 1/2008 on the transmission by Internet of information containing personal data

The current situation is one in which there is constantly increasing transmission of information of all kinds by electronic media, fundamentally Internet, which, since the information they transmit may well contain personal data on individuals, may affect the basic right to data protection.

The basic right to protection of personal information is enshrined in Article 18.4 of the Spanish Constitution and in Article 31 of the Catalan Statute of Autonomy as a right to information self-determination (STC 292/2000), and is developed in Organic Law 15/1999, of December 13, on the protection of personal data (LOPD). In accordance with this right, personal information can only be processed as is appropriate for achieving the legitimate ends justifying said processing and, in short, citizens should be able to know and exercise control over who uses their personal information, to what end and to whom this information is given, amongst other things. This control can be exercised through the so-called right of *habeas data* (right to access, correct, delete and object to information) which confers on the individual the power to protect this information and, therefore, to exercise effective control over it.

Regarding European provisions, we should mention Convention 108 of the Council of Europe, and the explanatory report to this Convention, according to which "information power' brings with it a corresponding social responsibility of the data users in the private and public sector". We should also mention the European Union directives that affect data protection, principally Directive 95/46/EC, and certain particularly relevant jurisprudential decisions such as the Decision of the European Court of Human Rights in Strasbourg, *Peck v United Kingdom*, of 28 January 2003, on the application of ECHR Article 8, or the Judgement passed down by the European Court of Justice on 6 November 2003 (*Lindqvist case*).

Bearing in mind, moreover, the status of public administrations and, at the very least, the links to the exercise of public functions that are shared by bodies subject to the Catalan Data Protection Authority's sphere of activity, we find that the right to personal data protection converges on another: the right of access to information recognised in Article 105 of the Spanish Constitution and developed by Law 30/1992, of November 26, on the legal status of public administrations and common administrative procedure, and in other dispositions concerning this sector in particular. In Catalonia, moreover, the Statute of Autonomy establishes citizens' right to access to information in areas with important effects on their lives, such as rights and responsibilities with regard to the environment (Art. 27.3), health rights (Art. 23.3) and the right of access to public services and to a good administration (Art. 30). This last right could also include access to necessary information about these public services as a measure of administrative transparency.

From the standpoint of personal data protection, the emergence of problems caused by the use of Internet to transmit information is further affected by two other

circumstances at present: firstly, the approval of Law 11/2007, of June 22, on citizens' computer access to public services; and, secondly, the approval of Law 2/2007, of June 5, on the Official Journal of the Autonomous Government of Catalonia (DOGC), according to which, from 30 June 2007 onwards, the digital edition of the DOGC is the only official version.

It is precisely the confluence of all these elements that has made it necessary to draft this Recommendation. The purpose of this text is not to introduce new legal provisions, nor even to provide an exhaustive memorandum on all data protection legislation, nor much less of all the legislation governing the sector that might affect the transmission of different types of data; it is intended only to serve as a memorandum on the most problematic aspects and, as far as possible, a tool for interpreting them. For this reason, having reviewed the most important principles applicable, we shall go on to discuss the problems that, based on the Catalan Data Protection Authority's experience, have been detected with regard to the transmission of data by bodies pertaining to this Authority's sphere of action, with particular emphasis (in a separate chapter) on the publication of data by electronic official journals.

However, the subject that concerns us here, the right to protection of personal data, also converges on other basic rights, particularly those recognised in Article 20 of the Spanish Constitution: freedom of expression and freedom of information. The recommendations made in this document are formulated with a view to creating a framework that guarantees full data protection, though if, in any particularly instance, this right should enter into conflict with another basic right, the different concurrent rights should be weighed up in order to find a solution that enables the satisfaction, as far as may be, of the interests involved without necessarily sacrificing the essential content of one basic right in favour of the other.

However this may, given the changing nature of technology and, in consequence, of the subject of the present initiative, this Recommendation is not conceived as a static measure, but as something more like a dynamic tool whose application the Catalan Data Protection Authority itself will ensure is subject to a constant verification process in order to monitor the results obtained from its application and to adapt its provisions to any new problems or circumstances that may arise.

According to Article 15 of Decree 48/2003, of February 20, approving the Statute of the Catalan Data Protection Authority, the Authority's director is responsible for establishing the instructions and recommendations necessary to adapt the processing of personal information to the principles laid down by current legislation with regard to data of a personal nature.

Chapter I. General considerations

1

OBJECT OF THE RECOMMENDATION

The object of this Recommendation is to provide guidelines for action with regard to the transmission of information containing personal data on Internet websites and webpages. The Recommendation is also applicable to the transmission of personal data by intranet or extranet, as established in Chapters I and II of this Recommendation, except as concerns Section 16.

When personal data is processed in ways involving the transmission of the information contained by Internet or a corporate intranet, all those responsible for personal data files subject to the control of the Catalan Data Protection Authority should bear in mind the considerations made in this Recommendation with regard to the principles and obligations established in current legislation concerning the protection of personal data.

The following aspects are excluded from the objects of this Recommendation:

- a) The transmission of information that does not contain personal data or which has been previously processed to ensure that the people concerned cannot be identified.
- b) Internet data gathering, which is governed by legislation on personal data protection and other applicable laws.
- c) The transmission of service information on people occupying certain posts within the body or authority, their functions and contact details when necessary according to these functions.
- d) Acts and dispositions that include only, with regard to personal data, the identification of the posts and public workers who drafted the acts or dispositions, or verify their authenticity.
- e) The transmission of information using systems that require identification prior to granting access, in order to check the necessary legitimacy of users to access personal data.

2

SCOPE

This Recommendation is addressed to all bodies, entities and authorities forming part of or attached to public institutions in Catalonia, the Autonomous Government, local authorities in Catalonia, the universities of Catalonia and public corporations that exercise their functions exclusively in Catalonia, and which come under the Catalan Data Protection Authority's sphere of activity according to Article 156 of the Statute of Autonomy of Catalonia, independently of the location of the information server and

whether the information transmitted by Internet is accessible by users in other countries.

The Recommendation also concerns public or private organisations that, in accordance with any contract, agreement or legal disposition, manage public services or exercise public functions, always on condition, in the latter case, that processing is performed in Catalonia and concerns issues falling under the powers of the Autonomous Government of Catalonia or local authorities in Catalonia.

3

CONCEPT OF TRANSMISSION

For the purposes of this Recommendation, transmission is considered to be the communication of information containing personal details by Internet, intranet or extranet, addressed to an indeterminate plurality of recipients without the need for prior identification on the part of those responsible for transmission to accredit the necessary legitimisation to access this personal data.

By “personal data”, we understand all information that identifies or makes it possible to identify an individual, as stipulated in the definitions established in Article 3 of the law on protection of personal information (henceforth, LOPD), and Article 2.a) of Directive 95/46/EC. Of particular interest for delimiting this concept here is the Report of 20 June 2007 by the Working Group on Article 2, with regard to the concept of personal data.

4

PRINCIPLES

Without prejudice to the general principles for procedure and the legal framework governing the public administrations and legislation governing the particular sector concerned, when transmitting information by Internet it is necessary to take into account the principles laid down in the legislation on personal data protection and, particularly, the following:

Consent: information containing personal data can only be transmitted with the consent of the data subject or when this transmission derives from the provisions of legislation in force.

Proportionality: this is a necessary consideration to ensure that the information provided is strictly appropriate and that it is displayed only during the time appropriate to achieve the object legitimising transmission of the data. Here, “appropriate” is considered to mean the information strictly suitable and necessary to achieve the object pursued, on condition that, when it is possible to transmit the information electronically in different ways, or at different levels of specificity, the system chosen is that which, whilst similarly permitting the achievement of the object pursued, entails the lowest level of personal data transmission from both a qualitative and quantitative standpoint.

Exactitude: the administration or body transmitting or order the transmission of personal data by Internet is responsible for ensuring that the data is correct and up to date, as well as for ceasing transmission when this becomes unnecessary or illegitimate.

Inalterable nature of rights and guarantees: guarantees must be provided when Internet is used to transmit information that all legal rights and safety guarantees are respected, as laid down in Law 30/1992, of November 26, on the legal status of the public administrations, in Organic Law 15/1999, of December 13, on personal data protection, and other applicable legislation.

Adaptability to advances: when transmitting information by Internet, it is essential to adapt security measures to technological advances and to the needs arising from new threats and dangers.

Responsibility: the bodies responsible for files or processing are responsible for the information containing personal data which is transmitted by Internet, irrespective of any responsibilities that may also attach to information society service providers or entities providing intermediary services with these.

Constant technological progress and advances means that the specific provisions described in this Recommendation may quickly lose their effectiveness in responding to the problems detected to date. For this reason, if, in the realm of data protection generally, it is important to ensure compliance with the principles established, fundamentally, by Article 4 of the LOPD, it is much more so in this sphere, since these are the general principles that will enable a response to be made to any new problems that may arise.

Chapter II. Transmission of information by Internet

Without prejudice to the considerations that follow with regard to electronic official journals and bulletins, we should remember that Internet and the websites of public institutions are not, in themselves, considered public access resources.

For this reason, the processing of data on Internet or the websites of public institutions is subject to the principles and guarantees laid down in the LOPD, applicable in all cases, according to the nature of the data concerned.

The transmission of information containing personal data via Internet by any of the bodies included in the scope of this Recommendation from a server located on Spanish territory does not constitute an international transfer of data, whether or not the

information can be accessed from third countries. Such transmissions are not, therefore, subject to legislation regulating international data transfers.

Section 1a: general conditions for transmission

5

LEGITIMACY OF PUBLICATION: *Transmit the information containing personal data only when you have the prior consent of the subject or when authorised by regulations with the status of law*

The transmission of personal data by Internet, even though it has no specific addressees, is considered as a communication of data as defined in Article 11 of the LOPD. Therefore, transmission by Internet of information containing personal data is only appropriate when carried out within the framework of the functions assigned to each of us, and requires either the consent of those concerned or authorisation by regulations with the status of law. In consequence, bodies responsible for files that contain such data are advised to make a prior analysis, from the personal data protection standpoint, of the information they plan to transmit in order to avoid transmitting information containing personal data other than as provided for under current legislation.

To this end, it is necessary, firstly, to consider whether the transmission of data may infringe individual rights and interests, particularly as described in Article 18 of the Spanish Constitution, taking into account the limits established by applicable legislation in the sector concerned, according to type of personal data, the individuals affected and whether access is provided to profiles on the personality or conduct of identified or identifiable individuals.

This consideration seeks to answer, at least, the following questions:

- Whether the data has been collected for a legitimate purpose and in a legitimate way.
- Whether the reservation of rights exists.
- Whether the data subjects have been informed about the subsequent transmission of their data via webpages, and the implications this may have.
- Whether consent has been obtained from the data subjects.
- Whether legal provisions exist regarding the publicity to be given to this information.
- Whether the data to be transmitted contains any information that should be considered as requiring particular protection or that refers to the individual's honour, privacy or image.
- Whether the data refers to minors or to people requiring special protection due to security or other reasons.
- Whether the data enables or facilitates access to profiles on the personality or conduct of the people concerned.
- Whether it is possible to manage access to the personal data using passwords or other systems that restrict access to the data subjects or to the sections on the webpage to which access is not open.

- Whether regulations stipulate a particular duration for publication of the data or, if not, what this duration should be.

The existence of particularly sensitive data may make it advisable to establish different sections on a webpage to enable access to be restricted to data so requiring.

In cases where the applicable legislation confers a margin of discretion for evaluating the need for transmission, the duty to justify the reason for public administration acts in accordance with Article 54.a) of the LRJPAC with regard to acts that restrict subjective rights. For this reason, it is recommended in such cases that the transmission should be preceded by a decision based on weighing up the duty of publication against the effects that this may have on the right to protection of personal data.

6

PROPORTIONALITY OF THE INFORMATION: Do not transmit more personal data than is necessary to achieve the purpose of transmission

In cases where the transmission of information is legitimate, the entity or body responsible is advised to adopt all possible measures to ensure that only the data strictly necessary in each case to achieve the purpose justifying this action is actually transmitted.

To avoid the unnecessary transmission of personal data, whenever it is possible to choose between different forms of publication, those responsible for the transmission are recommended to use that system which, whilst ensuring that the objective pursued is satisfied, best guarantees the right to protection of personal data. In consequence, in cases where, according to current legislation, the publication replaces or complements the notification of administrative acts containing personal data, the bodies that order its publication are advised to limit this to a brief indication of the contents and place of the act and the conditions in which interested parties may obtain full information on the act concerned, as long as this does not prevent the purpose of the publication from being achieved.

When the applicable legislation only provides for the use of Internet to provide certain data, though without specifying its public nature, those responsible are advised, as long as this does not prevent the purpose pursued from being achieved, to use access identification systems that enable verification of the legitimacy of those attempting to access the personal data to do so, to ensure that this data is transmitted only to those directly concerned or to individuals or groups with legitimate interests in this information.

In cases where there is no legal cover to justify publication, or where the end pursued can be equally achieved without the publication of personal data, those responsible are recommended to consider the possibility of making the transmission in such a way that anonymity is preserved, whilst informing interested parties as to how they can access

the full content of the act or information, or to use an access identification system as described in the previous paragraph.

Without prejudice to the possibility of using identifying numbers or codes to provide information in cases where such a system enables the end pursued to be achieved, it is also recommended that the publication of identifying numbers such as national identity numbers, social security codes, etc, accompanying the full identification of the person concerned should be limited to cases in which the publication of this specific information is required under the applicable legislation.

In cases involving the publication of results from selection processes or competitions, it is recommended that, unless the specific legislation regulating the subject stipulates otherwise, publication should be restricted to indicating the participants selected, without mentioning the scores obtained nor the participants rejected, without prejudice to the possibility of establishing restricted access systems enabling candidates to access all the information concerning them.

7

EXACTITUDE AND UPDATING INFORMATION TRANSMITTED: *Ensure that the data transmitted is correct and up to date*

The personal data transmitted must be correct. For this reason, we should avoid the transmission of partial or outdated information that could lead to mistakes or confusion and might cause harm to those affected.

Similarly, to avoid situations that might generate confusion, it is recommended that the publication of data on Internet should always be accompanied by information on the information was last updated.

8

TIME LIMIT ON TRANSMISSION: *adjust the transmission period to the time necessary to achieve the purpose pursued*

The principle of proportionality also requires that the transmission of data should be limited in time to the period required to achieve the purpose for which it is published.

To this end, it is recommended that bodies responsible for transmitting personal data by Internet should establish the necessary mechanisms to ensure that, once the period of public display determined by the law requiring its publication has expired, access to the personal data is restricted.

In cases where the applicable legislation does not expressly define a period for public display, then transmission should be limited in time to the period necessary to achieve the purpose for which the data is published, taking into account particularly to this effect, if the purpose of transmission is to ensure the transparency of the administrative action, participation in the formalities forming part of a procedure, the

efficacy of an act and the possibility of exercising the right of defence, amongst others.

Similarly, in cases in which transmission is grounded solely on the data subject's consent, the necessary measures must be adopted to cease transmission should the data subject withdraw this consent.

9

***PERIODIC REVIEW OF WEB CONTENT:** Make provision for periodic reviews of the data transmitted*

In order to achieve the purposes described in the previous two sections, it is recommended that periodic reviews should be carried out of website and webpage content (or at least those sections containing personal data), in order to correct any mistakes that may be detected and to cease transmission where this has become unnecessary or illegitimate.

10

***DUTY OF INFORMATION:** Inform about your privacy policy and on exercising rights*

Without prejudice to the duty of information established in Article 5 of the LOPD, it is recommended to provide information, on the site or page on which the data is transmitted, about the website's privacy policy (legal provision authorising the publication of data in each individual case, origin of the data, processing to which it is subjected, publication period established, use and storage of information about visits made, cookies, measures adopted to present certain types of search based on personal data, use of tools to enable third parties to process data traffic, etc). It is also recommended, especially, that users should be informed about the possibility of exercising their rights to access, correct, delete or object to the personal data transmitted, how to exercise these rights and whom they should address to this end.

11

***EXERCISING THE RIGHT OF HABEAS DATA:** Adopt appropriate measures to establish the right of habeas data*

The body or entity responsible for the personal data file in which the information is contained is also responsible for responding to applications seeking to exercise the right to access, correct, delete or object to data and, if necessary, for adopting the appropriate measures to put these rights into effect.

By exercising their right of access, interested parties can request that those responsible for the file containing the data published should inform them about the

origin of the data published, about other communications made or planned and about the purpose of the file containing this data.

By exercising their right of correction, interested parties can request those responsible for the file to correct any personal data that may be incorrect or incomplete. In this case, the data should be corrected and notice given on the site itself that this information has been rectified.

By exercising their right to object to the transmission of their data, the data subject can, unless a law to the contrary exists, prevent the transmission via Internet of certain data, or this transmission from taking place in certain conditions.

By exercising their right to delete data, the data subject can request, unless a law to the contrary exists, that their data, contained on one or more files, be removed from these files. This removal of the data entails the cessation of transmission of the data, though, in accordance with Article 16.4 of the LOPD, it is not necessary to notify those people who have already been informed of this by Internet.

12

***SECURITY MEASURES:** Adopt all necessary measures to protect the integrity of the data*

Those responsible for the website or page should adopt all necessary security measures to ensure the integrity of the information published, preventing it from being manipulated by third parties.

To this end, it is recommended that those responsible should introduce a system to identify web managers and editors in order to prevent manipulation of web content by unauthorised third parties.

Section 2a: Specific conditions

13

***LINKS TO OTHER WEBS:** Revise links to other webpages*

A specific problem arises with regard to information that may be disseminated indirectly by attaching links to other sites on the websites and webpages of the bodies that come under the scope of this Recommendation.

Although, in accordance with the provisions established by Law 34/2002, of July 11, on information society services and e-commerce (LSSICE), and by other applicable dispositions, it is the owners of sites themselves that are responsible for any liabilities arising from the transmission of the information contained on them, it is nevertheless recommended that links should not be provided to webpages that do not comply with

data protection legislation and with the recommendations established in this document.

14

***WEB HOSTING SERVICES:** Establish all necessary guarantees when hosting your site under third party servers*

When the person responsible for the file or data processing is not the same as the owner of the electronic medium used to transmit the data, it is recommended that all the obligations for which the service provider is responsible, resulting from the processing of personal data that they may carry out on behalf of the body responsible for the file, should be established, in detail, in the agreement or contract made previously, in accordance with Article 12 of the LOPD.

In such cases, according to the LOPD, those responsible for the file are also responsible for any liabilities that may arise from transmission of the data, without prejudice to any liability which may be incurred by the provider of the intermediate service, that of hosting on the server data provided by entities included within the scope of this recommendation, as established by the LSSICE and other applicable legislation.

15

***BLOGS AND DISCUSSION FORUMS:** Establish conditions in advance for use of the service*

When any of the bodies included in the scope of this Recommendation offer citizens the possibility of hosting, on their website or webpage, blogs or spaces where users can give their opinions or post any information they consider appropriate, and in those cases in which the possibility to take part in discussion forums is offered, those responsible for the website are advised to take the following measures:

- Establish the conditions for using the service, with particular emphasis on ensuring the impossibility of using this service to transmit personal data without either the consent of the persons affected or legal cover.
- Inform users of the service about these conditions appropriately.
- Require the establishment of identification systems to verify the identity of people posting the aforementioned opinions or information.
- Provide the necessary mechanisms to duly delete all personal data whose transmission is illegitimate.

SEARCH TOOLS: *Establish measures to restrict the misuse of search engines*

The transmission of data by Internet has made the use of search engines particularly important for looking for information on the Web. On this point, to give but one example, Law 37/2007, of November 16, on the reuse of information in the public sector, expressly establishes that administrations and public sector organisations should provide electronically accessible mechanisms to enable searches for available documents for reuse. However, this should not entail any watering down of guarantees regarding personal data on people who may be affected by this information since, as established in Article 4.6 in the same law, when documents contain personal data the provisions established by the LOPD must be followed.

The use of electronic media and, particularly, of search tools based on indexing webpage content, can allow information obtained using data mining techniques to be used for purposes other than those for which transmission is authorised. For example, such tools can be used to obtain personal profiles or indiscriminate information about a particular individual. For this reason, and without prejudice to any liabilities that may be incurred by the body providing the search tool, as established by the LSSICE, it is recommended that appropriate organisational and technical measures should be adopted to protect any personal data contained in such information. To achieve this objective, it may be appropriate to adopt one or more of the following measures:

- a. Carry out a prior study of the documents to be published in order to identify those that contain personal data.

- b. Adopt the technological measures necessary to prevent search engines from compiling personal data for purposes other than that for which they were published. To this end, the following technological measures are recommended:
 1. Use the tools provided by the search engines themselves to prevent them from temporarily storing data.
 2. Use technical protocols to prevent the indexing of documents containing personal data.
 3. Avoid using files to store the published personal data. Instead, use technical solutions based on structured information, such as databases, to access and store information.
 4. Consider the possibility of publishing the parts of files containing personal data as images or using other systems that restrict access to fields that contain such personal data.

17

THE TRANSMISSION OF PERSONAL DATA REGARDING INFRINGEMENTS, THE IMPOSITION OF PENALTIES AND COURT ORDERS: Avoid transmitting personal information about infringements, penalties or court orders without first anonymising the data, unless a law to the contrary exists

The transmission of personal data by Internet, and the resulting general and indiscriminate access to this data in the context of public administration sanctions and court orders, could harm or damage the rights of individuals alluded to in this information, and which goes beyond the penalty or court order itself. This would constitute, de facto, an additional penalty, one not provided for under the current legislation, particularly if the data can be located using search tools that enable different penalties or legal sentences to be linked.

Starting from the basis that personal data concerning infringements of legal or administrative regulations can only be placed on the files of the competent authority in cases provided for under their respective regulations, in accordance with the LOPD, in cases where those responsible for such files are considering the possibility of transmitting such personal information or the content of court orders, whether wholly or in partial form, the following points should be taken into account:

First and foremost, transmission must be legitimised by the exercise of the specific powers pertaining to the authority responsible for the webpage on which this information is to be published, and the purpose pursued by this transmission must be directly related to the specific exercise of these powers.

Moreover, transmission by Internet of personal information relating to legal, administrative or disciplinary infringements committed by a physical person must be expressly authorised by a regulation with the status of a law. Transmission is only permitted if such legal provisions exist, and must take place under the conditions established by these provisions. If the regulations do not specify transmission by electronic media, or if they leave the decision over which transmission media to use for this specific personal data up to those responsible, the latter should establish weighting criteria to evaluate in which cases electronic transmission is justified, whether by the issue concerned or because access to this data is in the collective public interest.

Regarding administrative infringements and penalties, clauses of a general nature that permit transmission should not be considered as providing sufficient cover to decide on this option to publish with absolute discretion; rather, the need for express provision indicates that the law itself should specify those infringements and penalties that can be transmitted in this way.

Legal sentences are not, in themselves, considered public access resources, and the conditions provided for in Article 6.2 of the LOPD are not, therefore, applicable to them. With regard to court orders, we should remember that, although court proceedings are public, with the exceptions established by the corresponding procedural laws, and that sentences must be handed down in public, Article 120 of the Spanish Constitution establishes that this principle of publicity should be interpreted

in its restrictive sense in order to protect the rights of people involved or directly or indirectly affected by this information. It is, therefore, unless the law establishes the contrary, necessary to obtain the unequivocal consent of those affected.

Unless the consent of those affected is obtained or authorised by legal provisions, the transmission of personal data in sentences declaring infringements or imposing penalties or court orders requires the anonymisation of the personal data, making it impossible to identify the data subjects.

It is also recommended that personal data should be anonymised when press clippings or news articles are transmitted on websites or webpages, if these include any of the content referred to in this section.

In any case, the existence of legal provisions for data transmission in this context waives the need to require the consent of those affected, but does not waive the requirement to comply with all other principles and obligations established under data protection legislation.

18

TRANSMISSION OF THE MINUTES OF COLLEGIAL BODY MEETINGS: Do not transmit such minutes if they contain personal data

Whatever the legal framework applicable to the publication of acts and agreements adopted, the minutes of collegial body meetings considered secret may not be transmitted by Internet. With regard to minutes from public sessions, these should not be transmitted if they contain personal data other than that identifying the members at such sessions, the official designated to take the minutes and any other individuals who may attend by reason of their post, unless otherwise authorised by law.

19

TRANSMISSION OF PERSONAL DATA IN THE FORM OF IMAGES OR VOICES: Consider whether transmission of such data is proportionate and legitimate

Transmission by Internet of images or voices that enable individuals to be identified requires the consent of the person concerned, unless cover is provided by the stipulations of Organic Law 1/1982, of May 5, on the protection of the right to personal honour, personal and family privacy and image, or by other regulations with the status of law.

For this reason, apart from the aforementioned circumstances, it is recommended that images, whether still or moving, should be transmitted only in cases where this is justified, after the proportionality of such a measure has been duly weighed up and, in any case, in such a way that particular individuals cannot be identified.

Nonetheless, images from the sessions of parliamentary bodies and the governing bodies of local authorities and collegial bodies can be transmitted when these sessions

are public, in accordance with their respective legal rules and regulations, as long as this does not infringe the privacy rights of third parties.

Chapter III. Publication in electronic official journals and bulletins

Without prejudice to whether the considerations formulated in the previous chapter of this Recommendation are applicable where the provisions in this chapter do not indicate otherwise, the considerations formulated in the following sections should be specifically taken into account with regard to publishing information containing personal data in official journals and bulletins.

20

SEARCH TOOLS: *Establish measures to restrict misuse of search engines*

According to Article 3.j) of the LOPD, official journals and bulletins are public access resources. This implies the possibility that the information contained in them may be consulted and processed by any individual, and that, in accordance with LOPD Article 11.2.b), the data contained in these media may be communicated to third parties.

This is really a special legal situation with notably higher possibilities for processing information than can be undertaken generally. However, the status of public access resources should not be taken to eliminate the guarantees attached to personal data on people who may be affected by this information. On the contrary, Article 6.2 of the LOPD itself establishes that such processing must respond to the legitimate interest of those responsible for the file or the third party to whom the data is transmitted and, in any case, must not breach the basic rights of the interested party.

For this reason, and also without prejudice to the liabilities that may be incurred by the body providing the search tool, in accordance with the provisions of the LSSICE, when information is transmitted through publication in official journals and bulletin, the following recommendations are made:

A) The bodies ordering publication should cooperate with those responsible for the official journal or bulletin to apply the measure provided for in Letter b), Section 16 of this Recommendation, identifying, as established by the body responsible for the official journal or bulletin, the documents or parts of documents that contain personal data.

Similarly, these bodies are responsible for preventing the inclusion of personal data in the titles of documents, unless necessary to achieve the purpose for which publication is made.

B) The bodies responsible for the official journal or bulletin should ensure that the measures described in Letter b), Section 16 of this Recommendation or other similar

measures enabling the same objects to be achieved, are effectively implemented. Similarly, they should establish mechanisms enabling the body responsible for the information to identify the documents or parts of documents that contain personal data.

All this must be without prejudice to the introduction of additional systems limiting the possibility of carrying out mass information searches based on personal data to the search applications provided by the body responsible for the official journal or bulletin.

21

DUTY OF INFORMATION AND EXERCISING THE RIGHT OF HABEAS DATA: Adopt the necessary measures to effectively enable citizens to exercise these rights

Without prejudice to the duty of information established in Article 5 of the LOPD, it is recommended that information should be provided on the website where the electronic official journal or bulletin is published, on the possibility of exercising the rights to access, correct, delete and object to the personal data published on it, as well as the body before which these rights can be exercised. The short periods allowed to exercise these rights, particularly as regards deleting and correcting data, make this information particularly important in enabling members of the public to address their complaints to the competent authority.

If the data subject exercises his/her right to access, correct, delete or object to their data before the body responsible for the official journal or bulletin in accordance with the conditions established by the LOPD to exercise these rights, the following points should be taken into consideration:

- If the rights are exercised with regard to files or the processing of personal data that do not obey orders for publication issued by other bodies or persons, but refer to other processing for which the same body responsible for the official journal is also responsible, then this body should respond to the complaint and, if necessary, adopt the appropriate measures within the terms established by law.

- If the rights are exercised with regard to files or the processing of personal information for which a third party is responsible, that is to say, a public body or private person or organisation that has prompted the publication of the data in the official journal or bulletin, then the body responsible for the official journal or bulletin should refer the complaint to the person or entity that ordered its publication as soon as possible, and always within the space of 10 days, at the same time informing the person or person concerned of this.

The body or entity that ordered publication is responsible for responding to applications to exercise these rights and, if necessary, for ordering the body that manages the official journal to implement the measures required in order to comply with the resolutions adopted.

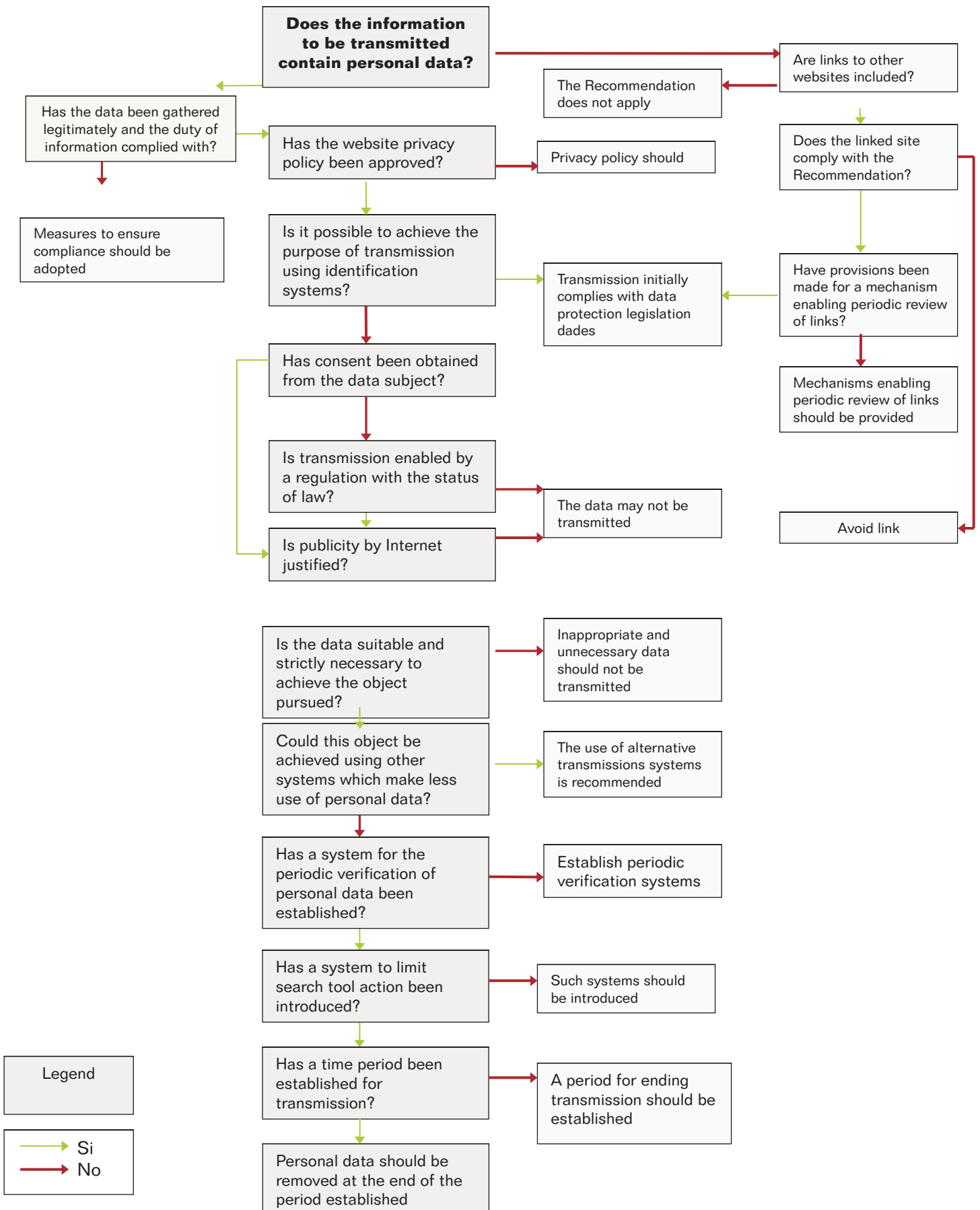
If the decision is taken that published data should be rectified, whether ex officio or as a consequence of a complaint from the interested party, those responsible for the file

must notify the body responsible for the official journal or bulletin of this rectification so that this body can publish said rectification and take the necessary steps taken to notify users about this in the information originally published.

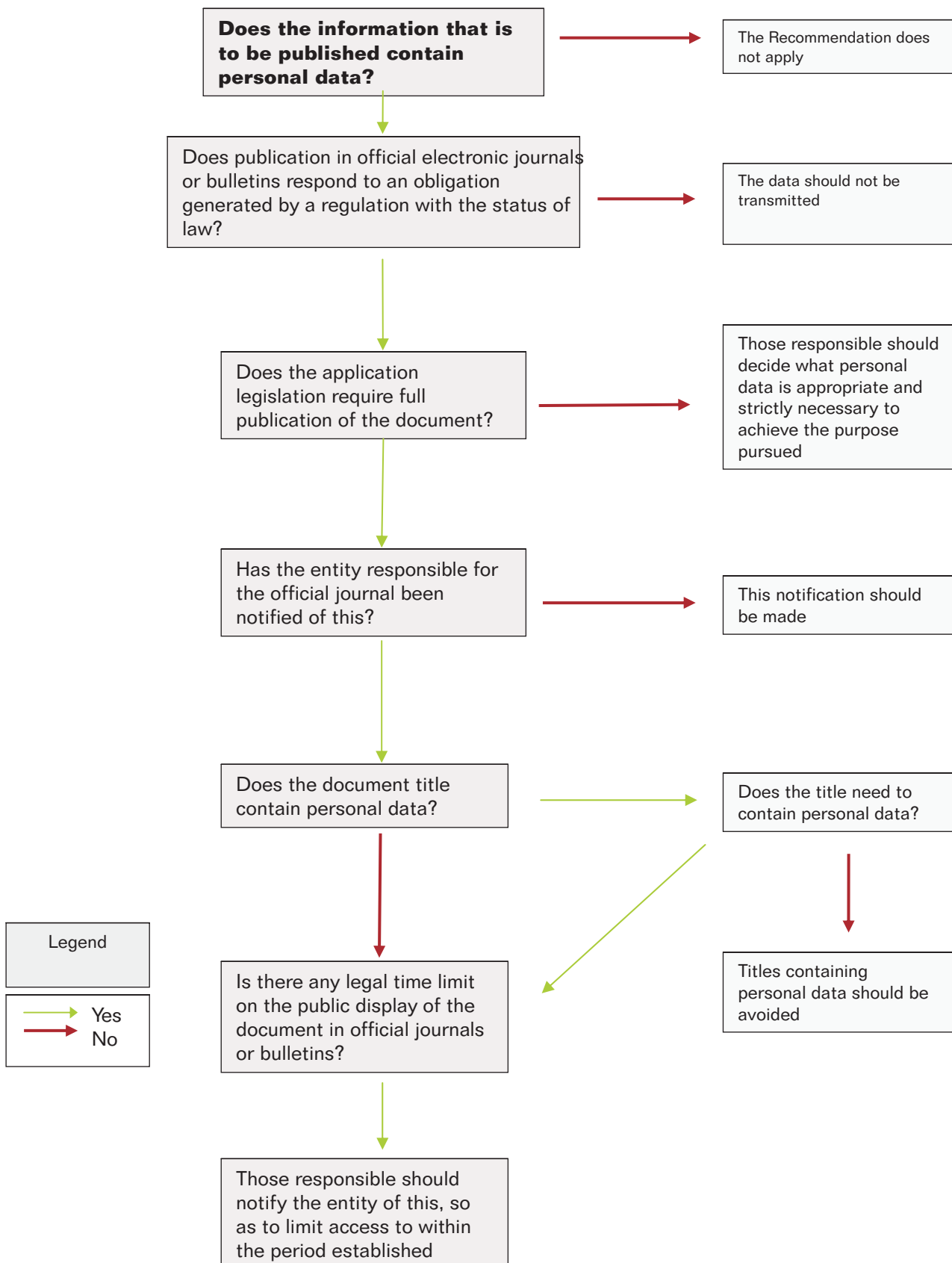
If it is agreed to delete data that has been published in an official journal or bulletin, those responsible for the file should notify the body responsible for the official journal or bulletin of this, since this body should also delete the data.

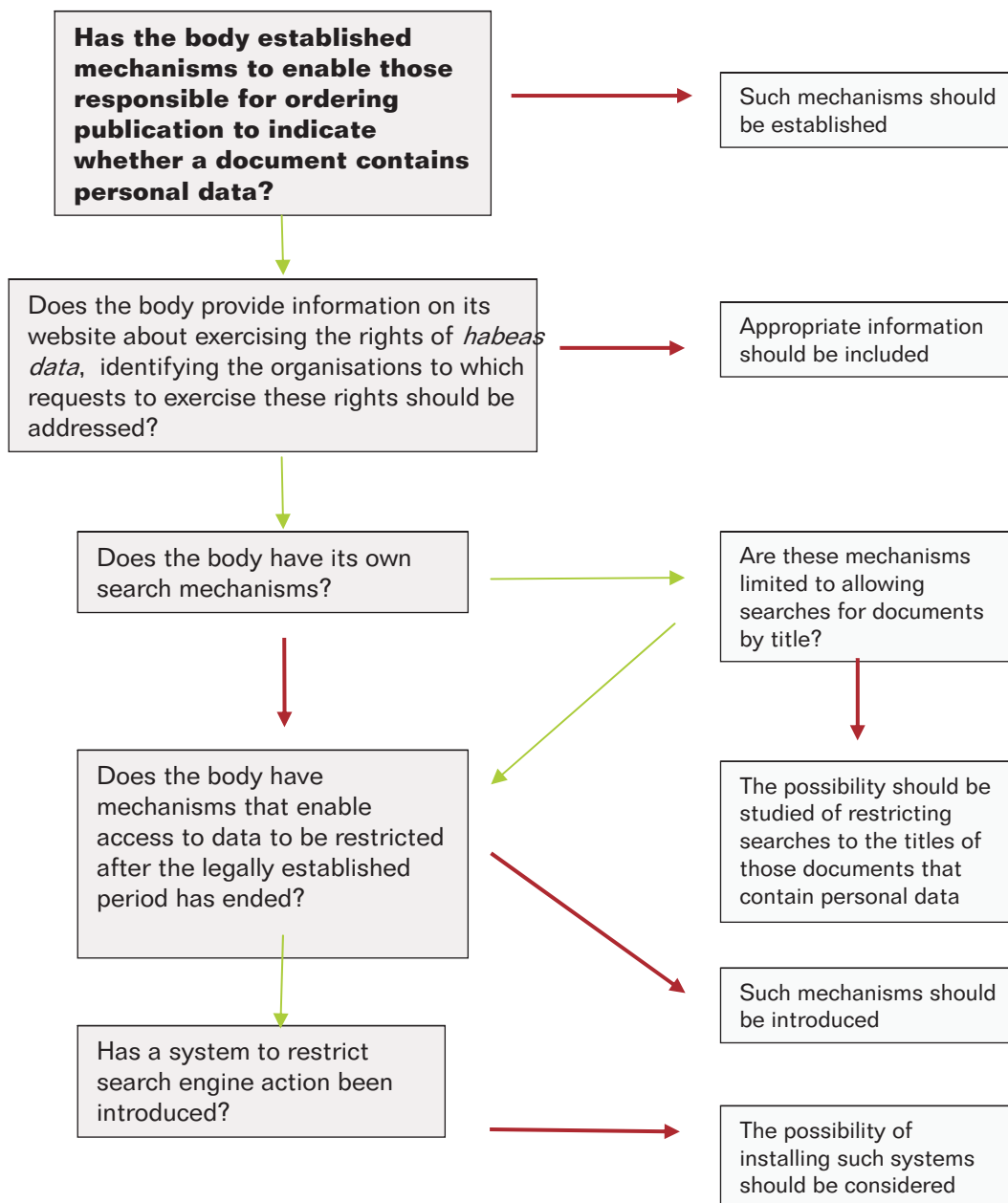
Barcelona, 15 April 2008

Esther Mitjans Perelló
Director



Guidelines for action by those responsible for ordering publication in official journals





Legend

→ Yes
→ No

