

LegalLeaks



A GUIDE FOR JOURNALISTS
ON HOW TO ACCESS
GOVERNMENT INFORMATION



The **Legal Leaks Toolkit** was prepared by Access Info Europe and the Network for Reporting on Eastern Europe n-ost.

The project was supported by the Representative on Freedom of the Media of the Organisation for Security and Cooperation in Europe.



This toolkit is part of the Access Info Toolkits series, a set of guides on how to exercise the right of access to information. The toolkit was devised by Helen Darbishire of Access Info Europe and Christian Mihr of n-ost. It was written by Helen Darbishire with input from Lydia Medland, Victoria Anderica and Pamela Bartlett of Access Info Europe. Further contributions were provided by Christian Mihr and Andrew Bock of n-ost. Thanks to all our partner organisations and users of the toolkit for their feedback.



This Legal Leaks Toolkit is published under a Creative Commons License which permits sharing and reuse, provided you attribute the source (Access Info and n-ost Legal Leaks Toolkit) and that you share it in the same way.



Access Info Europe is an international human rights organisation, based in Madrid, which promote a strong and functioning right of access to information in Europe and globally.

Access Info's works to make the right of access to information to serve as a tool for defending civil liberties and human rights, for facilitating public participation in decision-making, and for holding governments accountable.



The **Network for Reporting on Eastern Europe n-ost** (www.n-ost.de) links 250 journalists and media initiatives from more than twenty European countries and is based in Berlin. Members of n-ost are against any restrictions that limit journalistic endeavour. The focus of n-ost is on detailed reports from and about Eastern Europe and on organizing Europe-wide journalistic projects on the promotion of media freedom and a European public sphere.



The **OSCE Representative on Freedom of the Media** observes media developments in all 56 OSCE participating States. She provides early warning on violations of freedom of expression and promotes full compliance with OSCE press freedom commitments.

CONTENTS

Overview – Is this for me?	7
Twenty Top Tips for Busy Journalists	10
I. RIGHT TO INFORMATION & JOURNALISTIC RESEARCH	14
1. When is the right time to submit a request?	14
2. The newsroom culture for access to information	14
3. Information Requests and Spokespersons	15
4. Where should I submit my request?	16
5. Shall I let them know that I am a journalist?	17
6. What should I say in my request?	18
7. Hiding the “real request” in a more general one	20
8. Anticipate possible exceptions	20
9. What information about myself do I have to give?	21
10. How do I make my request?	22
11. Do I have to pay a fee to ask for information?	23
12. Fees for receipt of information	24
13. How will I receive the information?	25
14. When will I receive the information?	25
15. What happens if I don't get the information I asked for?	26
16. What do I do when I get the information?	28
II. STEP-BY-STEP GUIDE TO THE RIGHT OF ACCESS TO INFORMATION	30
1. What is access to information?	30
2. What is transparency? Is it the same as access to information?	31
3. I've been thinking: is access to information really a human right?	32
4. Who has the right to submit information requests?	34
5. Which information or documents does the right apply to?	36
6. What about access to an entire database?	37
7. Does the right apply to all public bodies?	40
8. What about inter-governmental organizations?	40
9. But can I get access to all information held by public bodies?	41
10. Appeals against silence and refusals	43
ANNEX A: Adoption of Access to Information Laws 1766-2010	47
ANNEX B: Access to Information Laws in the 56 OSCE Participating States	48
ANNEX C: The Scope of the Right of Access to Information	51
ANNEX D: Appeals Options and Oversight Bodies	53
ANNEX E: Access to Information Timeframes	64

OVERVIEW: IS THIS FOR ME?

This toolkit is designed for journalists working in any media – newspapers, radio, and television – as well as bloggers and other information professionals who need to get access to information held by public bodies for their stories.

The toolkit is for journalists making requests in their **own country** or considering submitting a request in **another country**. It is based on a comparative analysis of the access to information laws in the region covered by the *Organization for Security and Cooperation in Europe*, which has 56 participating states in Europe, Central Asia and North America; of these 45 have legal provisions on the right of access to information held by public bodies which are reviewed in this analysis.

Most of these access to information laws are in line with international standards but there are exceptions and in the text we indicate where national law or practice deviates from the standards. More information on national legal frameworks is given in Annex B.

In Annex C you will find information about the relevant oversight body (Information Commission or Ombudsman), where they exist; these oversight bodies should be able to provide more in-depth information about the national access to information framework and assist

requesters in their search for information.

Isn't this only for investigative journalists? No, all journalists can make use of the tool of access to information. Investigative journalists can make regular use of access to information laws and this toolkit will help anyone working on in-depth stories. At the same time, everyday stories such as a story about modernization of a local hospital or plans for the village school can be written with information obtained under access to information laws. Often these stories are as interesting to your readers, listeners, and viewers as a story about high level political intrigue or the fight against transnational organised crime.

Is this relevant to regional or local government? All government bodies hold information which is of some relevance to the public. Sometimes the most important stories come from what seem at first to be quite simple and straightforward questions posed to a local or regional authority.

Is this relevant if I am writing about the European Union or other International Organisations? The EU access to documents rules are covered in this Legal Leaks Toolkit and we make reference to where you can find information about the access to information rules of other intergovernmental bodies.

I work in TV, I need images! Most access to information or freedom of information laws apply to all information “recorded in any form” held by public bodies. That means that the right to information applies to audio visual material as well as to printed material. Documentary journalists can and do make use of this right to get images and audio-visual material for their stories.

I don't have much time, is this still relevant? One of the biggest concerns that journalists have about access to information laws is the timeframes: having to wait 15 or 20 working days for an answer is an awfully long time when journalists' deadlines come every day or even every hour. With this toolkit we show how submitting requests for information can be easy and fast, and once you have sent off a few requests, you can get on with other work while waiting for an answer. When the information does come, it might turn out to be an unexpectedly good story which was worth the wait.

Why bother? They are not going to answer my questions! It's surprising what information does get released under access to information laws so it's often worth a try. And even if you get a refusal or just silence, you can make a story out of that: the government is formally refusing to release information on a particular topic or failing to respond to citizens. Turning refusals into stories is explored more in Section I, Point 15.

Really, I don't think they will answer – can I submit requests in another country? Yes, most countries allow anyone to submit an access to information request. It is a useful way of getting comparative data on levels of transparency to press your government to answer.

If I start submitting formal information requests, it will ruin my relationship with the spokesperson! It's not uncommon, especially in the early years of an access to information law, for government officials to get angry with journalists who start submitting formal requests. This problem is considered more in Section I, Point 3 along with some strategies that you can use to get around this problem.

I don't think my bosses will like it if I start using the law – they might think I am threatening to sue government officials and they will have to pick up the costs. It is sometimes necessary to convince your colleagues that it's worth using access to information laws. We give you some suggestions on how to change the newsroom culture and its attitude to access to information laws in Section I, Point 2, along with some tips on what you can do in the meantime.

I am a foreign correspondent: can I still submit information requests? Yes, in most countries, the right to request information is a right for anyone. You may need to speak the language of the country however, but if you are based there, it's usually possible to find someone who can help you translate the request (see also next point).

I want to submit a request in another country but don't speak the language. In this case you should turn to the **Legal Leaks network** (you can find details at www.Legalleaks.info) which will help you find a journalist in the relevant country who can translate your request or even submit it for you. See Section II, Point 4.

I am interested in getting access to entire databases, is this possible? Increasingly it is possible to get access to entire databases rather than just some information extracted from them. This presents huge potential to journalists who are ready to explore the data they contain. You can read more about recent releases of government databases in Section II, Point 6. Contact the Legal Leaks team to find out more about opportunities for training on Computer Assisted Reporting techniques.

I am concerned about the security of my data. If you are collecting data from many sources, including public institutions and other research, the combination of the information can become highly sensitive. Requests to public bodies that are involved in corruption can trigger aggressive and illegal behaviour from officials. Journalists may have their phones tapped, computers hacked, may be followed, or be subject to other forms of harassment.

Part of this is the risk of being an investigative journalist. The risks should be considered carefully in each country and in each case. Good data security techniques help reduce risks. More information can be found in the complementary data security toolkit from the **Tactical Technology Collective** www.tacticaltech.org.

TWENTY TOP TIPS

A Quick Guide to the Legal Leaks Toolkit for Busy Journalists

1. Plan ahead to save time: Think about submitting a formal access request whenever you set out to look for information. It's better not to wait until you have exhausted all other possibilities. You will save time by submitting a request at the beginning of your research and carrying out other investigations in parallel.

2. Start out simple: In all countries, it is better to start with a simple request for information and then to add more questions once you get the initial information. That way you don't run the risk of the public institution applying an extension because it is a "complex request".

3. Submit multiple requests: If you are unsure where to submit your request, there is nothing to stop you submitting the request with two, three or more bodies at the same time. In some cases, the various bodies will give you different answers, but this can actually be helpful in giving you a fuller picture of the information available on the subject you are investigating.

4. Mention your right to information: Usually the law does not require that you mention the access to information law or freedom of information act, but this is recommended because it shows you know your legal rights and is likely to encourage correct processing of the requests according to the law. We note that for requests to the EU it's important to mention that it's an access to documents request and it's best to make a specific mention of Regulation 1049/2001. It is also recommended that you use language and etiquette appropriate to any other professional communication in your country.

Remember: There is also no need to say why you want the information, nor to answer questions about the reason for asking or what you will do with the information.

5. Tell them you are a journalist: If the law says only individuals can request information but you want to let the public institution know that you are a journalist, you could always write your request on your media organisation's letterhead. **BUT** before you do this you should be sure that this is acceptable with the organisation. Another option is to mention in the letter or e-mail that you are a journalist and/or who you work for.

6. ... or don't tell them that you are a journalist! If you send an e-mail from your work address, it will often be obvious that you are a journalist, e.g.: jsmith@dailytimes.com. If you don't want to give the game away, it might be worth using a different address, such as a gmail/hotmail/yahoo account.

7. Hide your request in a more general one: If you decide to hide your real request in a more general one, then you should make your request broad enough so that it captures the information you want but not so broad as to be unclear or discourage a response. Specific and clear requests tend to get faster and better answers.

8. Anticipate the exceptions: If you think that exceptions might be applied to your request, then, when preparing your questions, separate the question about the potentially sensitive information from the other information that common sense would say should not fall under an exception. Then split your question in two and submit the two requests separately.

9. Check the rules about fees: Before you start submitting a request, check the rules about fees for either submitting requests or receiving information. That way, if a public official suddenly asks you for money, you will know what your rights are.

10. Ask for electronic documents to avoid copying costs: To avoid costs for copying and posting information, mention in your request that you would prefer the information in electronic format. That way you will avoid paying a fee, unless of course the information is not available electronically, although these days it's usually possible to scan documents which are not already digitalised and then to send them as an attachment by e-mail.

11. Ask for access to the files: If you live near where the information is held (for example you live in the capital where the documents are kept), you can also ask to inspect original documents. This can be helpful when researching information that might be held in a large number of documents that you'd like to have a look through. Such inspection should be free of charge and should be arranged at a time that is reasonable and convenient for you.

12. *Keep a record!* We advise you to make your request in writing and to save a copy or a record of it so that in the future you are able to demonstrate that your request was sent, in case you need to make an appeal against failure to answer, for example. This also gives you some evidence of submitting the request if you are planning to do a story on it.

13. *Speed up answers by making it public that you submitted a request:*

If you write or broadcast a story that the request has been submitted, it can put pressure on the public institution to process and respond to the request. You can update the information as and when you get a response to the request – or if the deadline passes and there is no response you can make this into a news story as well. Doing this has the additional benefit of educating members of the public about the right of access to information and how it works in practice.

14. *Prepare to appeal against refusals and silence:*

Find out about appeals in advance, including the time-frame for presenting an appeal. If you are not sure what to do for the first stage of appeal, contact the office of your Information Commission/Commissioner or Ombudsman and they will be able to help you. If you don't have such a body, try phoning the institution which issued the refusal and asking them. If you still are having problems, then let Access Info know about it and we will try to help you, for example, by giving you the contact of an NGO or lawyer in the country.

15. *Make a story out of refusals:*

The refusal to release information following a request is often a story in itself. Be creative and constructive with the fact that the information was refused, get examples from other countries, ask experts what they already know, discuss the public interest in the information and try to use the story to press for greater transparency.

16. *Appeal based on the public interest:*

If you have been refused information that you wanted for a story you are working on, it might help to state in your internal administrative appeal that the information is needed for a media story and to state that there is a public interest in knowing that information. It's also important at this point to refer to your rights under the access to information law and/or constitution. (Of course, if you don't want the public authority to know you are working on a story, then don't mention it).

17. *Make a standard template for appeals:* Once you have drafted the first internal administrative appeal with references to the law and your rights, just keep the letter in your computer and you'll find that you have a template for future appeals. That will save you time as it should only need a little bit of changing depending on the content of the other requests. Examples of templates for your country can be found on the Legal Leaks Website www.legalleaks.info.

18. *Get help to address problems with spokespersons:* If you are finding that official spokespersons are angry at you for using the access to information law, then talk to the Legal Leaks team and/or your local access to information organisation or journalists' association. These NGOs might be able to raise your concerns and perhaps organise a training session for spokespersons to explain journalist's rights under the law. They should also be able to support you in your discussions with government about giving proper treatment to formal access to information requests submitted by journalists.

19. *Involve your colleagues in using access to information:*

If your colleagues are sceptical about the value of access to information requests, one of the best ways to convince them is to write a story based on information you obtained using an access to information law. Mentioning in the final article or broadcast piece that you used the law is also recommended as a way of enforcing its value and raising public awareness of the right.

20. *Submit international requests:*

Increasingly requests can be submitted electronically, so it doesn't matter where you live. Alternatively, if you do not live in the country where you want to submit the request, you can sometimes send the request to the embassy and they should transfer it to the competent public body. You will need to check with the relevant embassy first if they are ready to do this – sometimes the embassy staff will not have been trained in the right to information and if this seems to be the case, it's safer to submit the request directly to the relevant public body.

I. RIGHT TO INFORMATION & JOURNALISTIC RESEARCH

In this section we guide you through submitting a request step by step, taking into consideration some strategic and tactical approaches relevant to journalists who want to integrate use of access to information laws into their information-gathering work.

1. When is the right time to submit a request?

If you are thinking of presenting an access to information request to a government body, it might mean that you have already tried other ways of getting the information and been frustrated.

There are however occasions when you might not want to waste time with the other ways of getting information and you will go straight to submitting an information request:

- » You suspect that you won't get the information unless you use the formal legal mechanism of the access to information law
- » You think access to information is a really good thing and you want to defend the right by using your access to information law as much as possible!

TIP! Plan ahead to save time: *Think about submitting a formal access request whenever you set out to look for information. It's better not to wait until you have exhausted all other pos-*

sibilities. You will save time by submitting a request at the beginning of your research and then carrying out other investigations in parallel.

2. The newsroom culture for access to information

Does your media organisation already have a culture of using the access to information law to get information? If not, you might be the first person to start doing so and you might need to change the newsroom culture. In particular, you might need to persuade your editors and bosses that submitting and pursuing access to information is not a waste of time but is actually a useful part of your journalistic activity. We hope that some of the points mentioned in this Legal Leaks Toolkit will help you make those arguments.

If there seems to be a bit of resistance there are a few things that you can do which might help:

- » Take your time to inform your colleagues about the access to information law

and get support for building it into newsroom strategy before bringing it up in a meeting

- » Collect examples from your country or from other countries about how access to information can lead to strong stories and exclusives (see www.legal-leaks.info for more information on this)

- » Explain to your colleagues that access to information is not only for investigative journalists but for all reporters researching a story and for all types of media outlet

- » Organise a training session and invite experts from your local access to information organisation to explain to your colleagues how the access to information law works and to demystify it so that it is not seen as something which will be too time-consuming (contact the Legal Leaks team for more information and to identify local experts for the training)

- » Submit a few requests on your own initiative, and then write stories based on them. Share the experience with your colleagues and encourage them to try to use the access to information law

- » If you have foreign correspondents based in countries with strong access to information laws, talk to them about submitting some requests in those countries in order to get information and also to gather positive examples of how access to information laws can result in useful stories

TIP! Involve your colleagues in using access to information: *If your colleagues are sceptical about the value of access to information requests, one of the best ways to convince them is to write a story based on information you obtained using an access to information law. Mentioning in the final article or broadcast piece that you used the law is also recommended as a way of enforcing its value and raising public awareness of the right.*

3. Information Requests and Spokespersons

If you are planning to submit an access to information request to a particular public institution for the first time, you might want to consider your relationship with the spokesperson of that organisation. The job of the spokesperson is to put a spin on information and to maintain good relationships with journalists; they may see the submission of an access to information request as an aggressive move which undermines their authority.

Access Info knows of cases from Europe and Latin America where spokespersons have phoned journalists and complained in strong language about the fact that a request was submitted. Part of the complaint in one case was that the spokesperson would get into trouble with his bosses for not managing the media effectively.

So, depending on your relationship with the spokesperson, you might want to let them know that you plan to submit a request, explaining that it's your legal right under the law, and that it's a different process from getting a comment from the spokesperson. Or you may decide just to keep these arguments in your mind in case you do get that angry phone call!

Another problem is when the person processing the request realises that it counts from a journalist and passes it to the spokesperson rather than being processed as an access to information request. This should not happen and if it does you should complain to the public institution and make clear that you would like your request to be treated on an equal basis with other requests.

Talk to other journalists and find out their experiences of submitting requests and if they have had the problem of receiving complaints from spokespersons or of requests not being treated as ordinary access to information requests. If this seems to be a common problem you might want to consider raising it with your professional association and getting them to complain to the government or Information Commissioner or Ombudsman. You might also want to make a story out of it.

TIP! Get help to address problems with spokespersons: *If you are finding that official spokespersons are angry at you for using the access to information law, then talk to the Legal Leaks team and/or your local access to information organisation or journalists' association. These NGOs might be able to raise your concerns and perhaps organise a training session for spokespersons to explain journalists' rights under the law. They should also be able to support you in your discussions with government about giving proper treatment to formal access to information requests submitted by journalists.*

4. Where should I submit my request?

Once you know what you want to ask for you need to identify the relevant public institution. In most cases this will be obvious, but in some cases you might have a slight doubt, in which case it's worth checking on the websites of the relevant bodies to see which seems to be responsible for that area of activity. A quick phone call to each institution might clarify further. That way you can also check if the body is covered by the national access to information law in case you are not sure.

Remember: When you phone you don't have to mention that you are a journalist nor why you want the information, espe-

cially if you think that this might set some alarm bells ringing inside the institution.

TIP! Submit multiple requests: *If you are unsure where to submit your request, there is nothing to stop you submitting the request with two, three or more bodies at the same time. In some cases, the various bodies will give you different answers, but this can actually be helpful in giving you a fuller picture of the information available on the subject you are researching.*

TIP! For international requests, use the embassy: *If you do not live in the country where you want to submit the request, you can sometimes send the request to the embassy and they should transfer it to the competent public body. You will need to check with the relevant embassy first if they are ready to do this – sometimes the embassy staff will not have been trained in the right to information and it's safer to submit the request directly to the relevant public body.*

5. Shall I let them know that I am a journalist?

There are pros and cons to letting the authorities know that you are submitting the request as a journalist.

PROS	CONS
<p>More info: In some countries, journalists tend to get faster answers and more information than individuals – this is not how it should be, but it's a reality in practice and you could try to take advantage of this positive discrimination.</p> <p>Cheaper: In some countries journalists are entitled to information free of charge. This is the case in the USA, where search fees will be waived, and in Serbia, where journalists don't have to pay photocopying fees.</p> <p>Faster: In some countries journalists get preferential treatment and to be provided with information in a shorter timeframe than other requesters.</p>	<p>Refusals: Signalling that you are a journalist might increase resistance to providing an answer out of fear that the information will be used in a critical story.</p> <p>Data Destruction: Signalling that you are a journalist might encourage public officials to hide or even destroy information in order to cover up corruption or other wrongdoing.</p> <p>Losing the story: If the records of requests submitted are public in your country (in some countries they are posted on line), then asking requests as a journalist might tip off other journalists that you are on to a story.</p>

I am not a lawyer: Do I need to read the access to information law?

Not really. The most important thing is to know how to file a request. A local access to information expert can tell you that. That said, it can be useful to look at the access to information law so that you know the basic elements and what it covers. You may also want to check the implementing regulation to see how the mechanisms for filing requests are defined. In addition – or as an alternative if you don't really enjoy reading laws – you can find an expert who will tell you how to file a request. On the **Legal Leaks website** you will find detailed information on how to file a request in each country, as well as copies of the laws and links to experts you can contact for assistance.

TIP! Tell them you are a journalist: *If the law says only individuals can request information but you want to let the public institution know that you are a journalist, you could always write your request on your media organisation's letterhead, if this is acceptable with the organisation. Another option is to mention in the letter or e-mail that you are a journalist and/or who you work for. ... or don't tell them that you are a journalist: if you send an e-mail from your work address, it will often be obvious that you are a journalist, e.g.: jsmith@dailytimes.com. If you don't want to give the game away, it might be worth using a different address, such as a gmail/hotmail/yahoo account.*

6. What should I say in my request?

We recommend that your request be clear and specific about the information or

documents you are looking for. In most cases it is not required by law to identify a specific document by any formal reference (Italy is an exception to this rule). At the same time, try to have in mind the job of the public official who has to answer your request: the clarity of your request will help him or her identify the information you need. A well-formulated request also gives public authorities fewer reasons to reject your request for not being clear (although as we noted, in most laws public officials have a duty to clarify the request).

In the first requests you send, it's a good idea to keep the requests relatively simple and not ask for huge volumes of information nor include multiple requests in the same letter. That way you have a better chance of getting a quick answer and you can always make follow-up requests if necessary. If you have a lot of requests, you might want to submit a series of

requests broken down by subject: this also helps the public institution forward the requests internally to the relevant departments so that they can prepare the response.

It is also recommended that you use language and etiquette appropriate to any other professional communication in your country.

Here is an example of a typical access to documents request:

Dear Sir/Madam

I am writing to request under the Law on Access to Administrative Documents (1996), copies of the minutes of the meeting at which the decision was taken to grant planning permission for the construction of a new hotel on the site of the old park.

I would prefer to have this information electronically sent to my e-mail address which is given below.

If you have any questions or need to clarify this request, please do not hesitate to contact me.

Yours faithfully,

Jane Smith

15 Old Town Street, Capital City

e-mail: jane@janesmith.com

Here is an example of an access to information request:

Dear Sir/Madam

I am writing to request the under the Law on Access to Information (2004) the total spent by the Ministry on the purchase of new colour printers in the financial years 2007 and 2008.

I would prefer to have this information electronically sent to my e-mail address which is given below.

If you have any questions or need to clarify this request, please do not hesitate to contact me.

Yours faithfully,

Jane Smith

15 Old Town Street, Capital City

e-mail: jane@janesmith.com

TIP! Mention your right to information: Usually the law does not require that you mention the access to information law or freedom of information act, but this is recommended because it shows you know your legal rights and is likely to encourage correct processing of the requests according to the law. We note that for requests to the EU it's important to mention that it's an access to documents request and it's best to make a specific mention of Regulation 1049/2001. The name of your national law can be found in Annex B.

Remember: There is also no need to say why you want the information, nor to answer questions about the reason for asking or what you will do with the information.

7. Hiding the “real” request in a more general one

If you are concerned that your request might indicate to the public institution that you are working on a particular story or looking for particular information, you might want to “disguise” your request by asking a more general question.

So, for the sample requests we gave above, you might want to change it to something more general, for example: “Copies of the minutes of all planning committee meetings held between July and September 2009” or “The expenditure reports for the Ministry’s purchase of IT equipment (including computers and printers) for the years 2007 and 2008.”

TIP! Hide your request in a more general one: If you decide to hide your real request in a more general one, then you should make your request broad enough so that it captures the information you want but not so broad as to be

unclear or discourage a response. Specific and clear requests tend to get faster and better answers.

8. Anticipate possible exceptions

Ask yourself if any of the information you are looking for might fall under one of those exceptions listed in Section II., Point 9. Sometimes exceptions will be invoked because the information you are asking for is politically sensitive.

Ask yourself: Could the public body try to restrict access to that information by applying one of the exceptions?

Even if the answer to this question is “Yes” don’t be put off by the exceptions. The experience in many countries is that things which you expect will be refused are released – and things you expect will be released are refused! You can find **case studies** about this on the **Legal Leaks Website**. So it’s worth asking

for the information, but it’s important to do so in a way which will increase your chances of getting some information, as we explain here.

TIP! Anticipate the exceptions: If you think that exceptions might be applied to your request, then when preparing your questions, separate the question about the potentially sensitive information from the other information that common sense would say should not fall under an exception. Then split your question in two and submit the two requests separately.

For example: you want to ask about spending on new equipment for helicopters. You can split this into one question on how much was spent, and a separate request about what it was spent on (e.g.: which types of missiles were purchased). If the details of **what** was purchased are denied, at least you have a chance of getting the information on **how much** was spent.

TIP! Make it public that you have submitted the request: Another strategy which journalists can use to avoid refusals is to write or broadcast a story that the request has been submitted. This can put pressure on the public institution to process and respond to the request. **For example:** if your radio station is following a controversial story about a shortage of medicines in a local

hospital, when you submit the request for information about the spending on medicines, you might want to announce this on air and also post news about the request on your website. You can update the information as and when you get a response to the request – or if the deadline passes and there is no response you can make this into a news story as well. Doing this has the additional benefit of educating members of the public about the right of access to information and how it works in practice.

9. What information about myself do I have to give?

Your name and address are usually required, and it’s a good idea to give your e-mail address if you want the information electronically or if you live outside the country where you are requesting the information so that the public officials can be in touch with you.

It’s also a good idea to give a phone number in case the public official wishes to contact you to clarify your request: that could speed up the process of getting the information.

In some countries there is no obligation to identify yourself with a real name (i.e. pseudonyms and anonymous requests permitted). We advise you to provide a name and some address or contact details so that there is no obstacle to receive the

information or documents requested or in case the public authority needs any clarification to answer your request.

TIP! Visit the public body to inspect the files: *If you live near where the information is held (for example you live in the capital where the documents are kept), you can also ask to inspect original documents. This can be helpful when researching information that might be held in a large number of documents that you'd like to have a look through. Such inspection should be free of charge and should be arranged at a time that is reasonable and convenient for you.*

10. How do I make my request?

In general, to submit a request is simple and there are not many formalities. Requests can always be submitted in writing. This generally means either sending by post or hand-delivering a

written request to the public institution. In many countries you can also present requests by e-mail. A list of countries which permit e-mail requests is given in the Box A below. Note that in some cases e-mail requests are a matter of practice rather than law (Netherlands, Serbia). In other countries requests can be submitted via web-based forms (this system is used in Turkey for example).

In the case of oral requests you can do them either by phone or in person. The practice is quite varied on this although in some countries it is permitted by law. Note, however, that in some of these countries (Slovenia) the request is not seen as formal for the basis of a legal appeal. In other countries (Armenia, Romania) the rules are different for oral and written requests. It is therefore recommended that requests be submitted in writing in order to have a record of the request in case an appeal is necessary.

BOX A: Oral Requests and E-mail Requests

Oral requests	Email requests
Albania, Armenia, Austria, Azerbaijan, Bulgaria, Denmark, France, Germany, Hungary, Macedonia, Moldova, Netherlands, Romania, Serbia, Slovakia, Slovenia.	Armenia, Austria, Azerbaijan, Belgium, Bulgaria, Croatia, Denmark, Finland, France, Germany, Hungary, Macedonia, Moldova, Montenegro, Netherlands, Romania, Serbia, Slovenia, Sweden, United Kingdom + European Union

We advise you to make your request in writing and to save a copy or a record of it so that in the future you are able to demonstrate that your request was sent, in case you need to make an appeal against failure to answer, for example. This also gives you some evidence of submitting the request if you are planning to do a story on it. There are a number of ways that you can do this:

- » If you deliver the request by hand, take two copies and get one of them stamped
- » If you send it by post, we suggest using recorded or registered mail
- » If you send an e-mail, do it with an automatic “return receipt”, but be aware that in many countries this is not yet a legal proof like a formal record of delivery by mail – and some people switch off that function on their computers
- » It is also worth checking what the law is in your country: Is a simple e-mail a legal document? Is there a system for electronic signatures?

TIP! Use the copy. *You might want to scan a copy of your request before posting it or scan the request that has been submitted which has the official stamps on it. This makes a good image to illustrate your story and to post on your website.*

Formal Acknowledgements: In some countries public authorities are required under the access to information law to

issue a reference number to confirm that they received a letter or e-mail. This is the case, for example, at the EU level.

11. Do I have to pay a fee to ask for information?

Submitting your request for information should always be free of charge. The right to submit requests free of charge is confirmed by the Council of Europe Convention on Access to Official Documents, which permits requests only for the costs of copying and delivery.

The majority of countries comply with this rule. There are however a few exceptions:

» In **Ireland** a fee may be charged, which is generally €15 per request. An internal review appeal is €75 and the fee for an appeal to the Office of the Information Commissioner is €150. In addition, the search for the information may be charged at €20.95 per hour, although this fee will be waived if the information being requested would help a group or individual understand an issue of “national importance”. Fees will not be charged if the cost of collecting them will be more than the fee itself.

» In **Germany** a fee of between €30 and €250 may be charged, and if the authority has to carry out significant work in answering the request (for example for blacking out sensitive information) this can rise to as much as €500.

However, according to the Fees Regulation (Informationsgebührenverordnung) the fee (but not the additional costs) can be reduced by half or completely omitted on grounds of public interest.

» In **Canada** there is a \$CA 5 fee that must be sent with each request (and which is refunded if the information which answers the requests cannot be found).

For the remainder of countries in the Council of Europe region, submitting a request should be free of charge. If a public official tries to charge you, this is an abuse of office and should be denounced – or it could make a good story!

TIP! Check the rules about fees: *Before you start submitting a request, check the rules about fees. That way, if a public official suddenly asks you for money, you will know what your rights are.*

12. Fees for receipt of information

It is quite usual that national access to information laws allow public institutions to charge requesters for charges for the photocopying and postage costs related to answering requests. In many cases, if the answer is just a few pages, there will be no charge. In Estonia the law provides that the first 20 pages shall be free of charge. Electronic delivery of informa-

tion is normally free of charge.

In some cases you will be asked to pay for receiving information in another format (like copies, DVDs, etc.) and in these cases the authority should only charge you the official cost of copying or of reproduction of the information into any given format, as well as the cost of the material (DVD, CD).

This is something which is also endorsed by the **Council of Europe Convention on Access to Official Documents** which states at Article 7: *A fee may be charged to the applicant for a copy of the official document, which should be reasonable and not exceed the actual costs of reproduction and delivery of the document. Tariffs of charges shall be published.*

Note: The fee charged for photocopying, postage or for materials such as a CD or DVD should be in accordance with already published official rates. If you suspect you are being charged too much, raise a concern with the public body and/or with the Ombudsman or Information Commissioner.

TIP! Avoid copying costs: *To avoid copying costs, mention in your request that you would prefer information in electronic format. That way you will avoid paying a fee, unless of course the information is not available electroni-*

cally, although these days it's usually possible to scan documents which are not already digitalised and then to send them as an attachment by e-mail.

13. How will I receive the information?

You can get access to the requested information in different formats, including:

- » inspection of originals
- » photocopies sent by post or collected
- » e-mails
- » attachments to e-mails
- » DVDs or CDs

In almost all cases you can specify the format you prefer and you have a right to receive the information in that format, unless it is impossible or too expensive. For example, the cost of transcribing a police training video is high and so it is unlikely that you would receive a transcript even if you requested it, but you should be able to get a copy of the video in any case.

TIP! State which format you prefer. *In your request state politely but firmly which format you prefer. If you want information electronically, make sure to give your e-mail address. The advantage of electronic information is that it usually saves you from paying the photocopying and postage fee, and delivery of the information is often faster.*

14. When will I receive the information?

Around Europe there is a huge range of timeframes for answering requests and for providing information, and for notifications of extensions or for the issuing of refusals. The average is about 15 working days, or about 3 weeks. See Annex E for more details.

The countries with the **shortest response periods** are Norway and Sweden where the access to information laws do not establish a time frame but, in practice, requests should be answered within about 1-3 days. In Sweden requests should be answered “immediately” and in Norway administrative silence can be appealed after 2 weeks. At the other end of the scale, in Albania public institutions have 40 days to respond and in Austria the law establishes an eight week (60 calendar day) timeframe. Another exceptionally long timeframe is Spain, which does not have an access to information law but where the administrative law gives public authorities 3 months to respond to requests for access to public archives and registers.

The **European Union Regulation 1049/2001** establishes 15 working days for responding to requests; an extension of up to 15 additional working days may be applied in “exceptional cases, for example in the event of an application

relating to a very long document or to a very large number of documents.”

Note: Under the Aarhus Convention rules, the timeframe for providing environmental information is one month. You will need to check your national law to see if there is a specific timeframe for environmental information.

Extensions in case of complex requests: Most countries permit public bodies to extend the timeframes for a few days or even up to a month if the request is particularly complex. In all cases the requester should be notified of the delay and the reasons should be given. More details are found in Annex E.

TIP! Start out simple. *In all countries, it is better to start with a simple request for information and then to add more questions once you get the initial information. That way you don't run the risk of the public institution applying an extension because it is a "complex request".*

15. What happens if I don't get the information I asked for?

There are a number of ways in which you can be disappointed with the answer to an information request:

» You only get part of the information you asked for (but no formal refusal) - this is called an “incomplete answer”

- » You are told that the information “is not held” by that government department
- » You are granted partial access but some information is withheld on the basis of exceptions
- » You are refused access to all the information or documents that you asked for
- » You don't get any reply at all (“administrative silence” or a “mute refusal”)

In all these cases you have a right to appeal. The mechanisms for appeals are discussed in Section II, Point 10 and the chart in Annex D.

Before appealing an **incomplete answer** check that your question was in fact clear enough or whether it was possibly open to misinterpretation. If you think that it was not clear, then you might want to go back to the public body informally and try to clarify.

In the case of an **information not held answer** you need to check if you think the answer is credible. If you think that the public body does hold the information but maybe does not want to answer your request (or maybe just that the public official was badly informed themselves) then you could decide between an informal or formal appeal. It might be worth trying an informal clarification about what you wanted before launching a formal appeal. If, however, you think that there was deliberate obstruction going on, a formal appeal is recommended.

In the case of **partial access, full refusal or administrative silence**, the best option is often to appeal. The first stage is to appeal to the body which refused to give you the information or which failed to answer you. You should check what your national access to information law says, but normally the appeal letter can be sent to the head of the institution. In countries which have good access to information laws, there will be a simple and clear system for submitting appeals. The second stage of appeal is either to the courts or – if your country has one – the Information Commission or Commissioner, or the Ombudsman.

TIP! Find out about appeals in advance. *If you are not sure what to do for the first stage of appeal, contact the office of your Information Commission/Commissioner or Ombudsman and they will be able to help you. If you don't have such a body, try phoning the institution which issued the refusal and asking them. If you still are having problems, then let Access Info know about it and we will try to help you, for example, by giving you the contact of an NGO or lawyer in the country.*

Making a story out of refusals. The refusal to release information following a request is often a story in itself. In the UK, the government's refusal to release legal advice relating to the Iraq War was a story that ran and ran. The reluctance

of the UK Parliament to release MPs expenses in spite of court rulings to do so was also an ongoing story – and when the information was eventually leaked it was a major scandal which caused quite a few members of parliament to resign, resulted in an order to MPs to pay back a total of as much as €1.5 million ... and sold a lot of newspapers in the meantime!

Check list before writing a story about incomplete answers and refusals:

- » Look carefully at the request to see whether it was clearly worded and whether the public authority might have misunderstood what you were asking for: you don't want to criticise a public body for failing to answer a request that was badly written or confusing. If you are not sure, ask a couple of your colleagues
- » Check carefully which information you were given (if any) as well as what you were refused. That way you can make a clearer story focusing on what the government is actually refusing to provide
- » Be very clear if you are planning to appeal or not: it's not clever to state in an article or on the air that you are planning to appeal against a decision and then to do nothing – public authorities will get used to the empty threats and may be even less inclined to grant information in future if they think that they can get away with it. You may need to discuss with your media organisation's lawyers before you take a decision on whether or

not to appeal, or talk to a specialist access to information organisation.

TIP! Appeal based on the public interest: *If you have been refused information that you wanted for a story you are working on, it might help to state in your internal administrative appeal that the information is needed for a media story and to state that there is a public interest in knowing that information. It's also important at this point to refer to your rights under the access to information law and/or constitution. (Of course, if you don't want the public authority to know you are working on a story, then don't mention it).*

TIP! Make a standard template for appeals: *Once you have drafted the first internal administrative appeal with references to the law and your rights, just keep the letter in your computer and you'll find that you have a template for future appeals. That will save you time as it should only need a little bit of changing depending on the content of the other requests.*

16. What do I do when I get the information?

You write your story! You now have a pile of information. It's probably not your only source for the story, but you have a strong story with documentary evidence to support it.

You might use only part of the information you received in this story – some of it may be background information that you save for future reference. That's ok – you don't have to reproduce all the information received in your story if it is not interesting or relevant.

Sometimes the story will focus on what is missing from the information you received. For example, if the government is developing a new policy for the amount of money hospitals can spend on a certain drug, and they have told you that they don't have the information on how much was spent on that drug in each of the past 5 years, your story might be to question how the policy is being developed.

TIP! When you get the information, think laterally. *What does the information tell you? What is missing? If you were a government decision-maker, would the information be enough to take fact-based decisions? Your story can be about what is missing as well as what is there.*

Journalists in countries with strong access to information laws often **mention the right of access** to information in their stories. For example, they will say “Using information obtained under the freedom of information act ...” You can find examples of such stories on the website of the UK's Campaign for Freedom of Information (www.cfoi.org.uk).

The reasons for mentioning the use of the access to information law include:

- » Your story looks more credible if you state how you got the documents
- » You encourage public officials to implement the law
- » You make it harder for the government to refute your story
- » You encourage other journalists to use the access to information law
- » You raise public awareness of the right of access to information and so defend everyone's right to know

Although journalists have a tradition of using secret sources inside government (which you will probably continue to do because you will never get all the information you need with an access to information law), it is now good journalistic practice to make use of an access to information law.

TIP! Mention the Right to Information in your stories. *Defend your right to information by letting the public know about the existence of the access to information law and how it is and is not working.*



A good place to find out more about the law on access to information and your legal rights is a national access

to information organisation. The Freedom of Information Advocates Network has over 180 members worldwide.

See www.foiadvocates.net

Legal Leaks Help Desk: The Legal Leaks team has lawyers and experts in the right of access to information ready to help you with your access to information requests. If you have submitted a request for information and it has been ignored or denied, we'd like to hear about it. We will try to find a way to help you, for example by giving you advice on how to appeal or finding an access to information expert or lawyer in your country.

Write to the Legal Leaks Help Desk - helpdesk@legalleaks.info

II. STEP-BY-STEP GUIDE TO THE RIGHT OF ACCESS TO INFORMATION

1. What is access to information?

The principle behind the right of access to information is that public bodies are elected by the people and sustained by taxpayers' funds, so the public should have a right to know how that power is being used and how that money is being spent.

The Government's Duty: To Publish and to Answer: This right of access to information places two key obligations on governments:

First, there is the obligation to publish and disseminate key information about what different public bodies are doing.

Second, governments have the obligation to receive from the public requests for information and the obligation to respond, either by letting the public view the original documents or by sending them copies of documents and information held by the public bodies.

Many countries around the world have now adopted access to information laws to give effect to the right of access to information. The first law was the

Access to information is a right with two parts to it:

I. Proactive

The positive obligation of public bodies to provide, to publish and to disseminate information about their main activities, budgets and policies so that the public can know what they are doing, can participate in public matters and can control how public authorities are behaving.

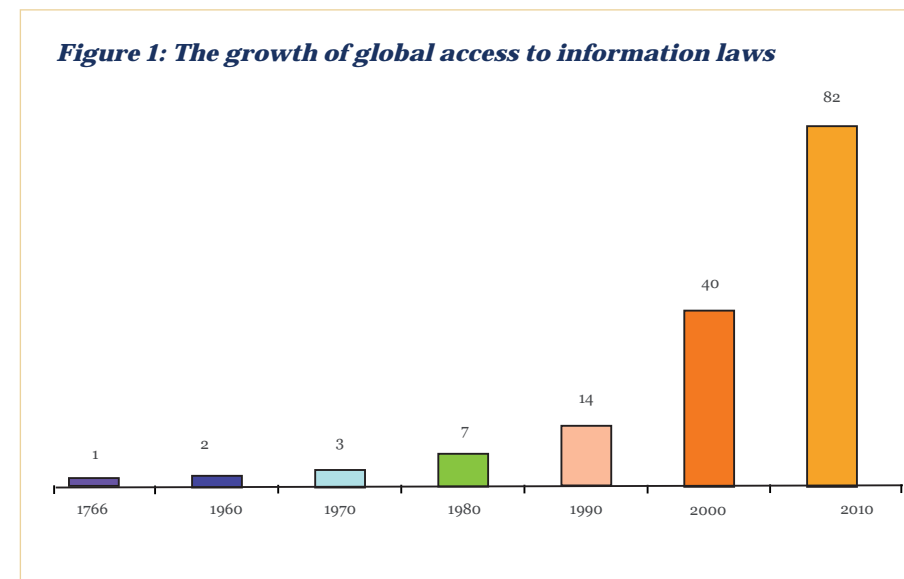
II. Reactive

The right of all persons to ask public officials for information about what they are doing and any documents they hold and the right to receive an answer. The majority of information held by public bodies should be available, but there are some cases where the information won't be available in order to protect privacy, national security or commercial interests.

Swedish law in 1766, but after that it took a while for the idea to catch on: Finland adopted its access to information law in 1951 and the United States in 1966. There was a small but steady growth in laws

during the 1970s and 1980s but the real expansion was after 1989 when civil society groups in central and eastern Europe started claiming this right as part of the shift of power during the post-Communist transitions.

Figure 1 shows how the number of laws regulating the right of access to information has grown significantly in recent years. It shows the total number of laws in a series of years from the world's first law (Sweden, 1766) through to the most recent laws to enter into force (Russia, January 2010). More details of the laws and dates can be found in Annex A and Annex B.



2. What is transparency? Is it the same as access to information?

People often talk about access to information and transparency in the same breath, but what is the difference?

A government is transparent when the great majority of the information that it

holds about its activities, policies, etc., is available to the public. Therefore, **transparency** is the result of information being available.

A transparent public body is one that is characterized by visibility or accessibility of information by people. Usually, this means not only that the public body

is good and fast at answering requests for information from the public, but also that they publish a large amount of information without the need for requests, for example by publishing on their internet site and in official journals as well as in user-friendly leaflets and reports.

It doesn't really matter too much if the words "transparency" or "access to information" are used, as the result is similar, but it helps to be specific.

Transparency has numerous benefits:

Transparency for accountability: The public has the right to hold the government and public officials accountable for their actions and for the decisions they take. To do this, information is needed. The role of the media is particularly important here because journalists play the role of "public watchdogs" – something which they have a right to do as confirmed repeatedly by the European Court of Human Rights.

Transparency for participation: In a democracy it is essential that people can access a wide range of information in order to participate in a real and effective way in the matters that affect them. That means not just participating in elections but also participating in public debate and decision-making between elections, and in order to participate in a meaningful way we need information.

Transparency for efficiency: Responding to requests for information also has the benefit of encouraging public institutions to organise their information. In particular, proactive disclosure of information encourages better information management. This in turn should result in better, more fact-based decision-making inside each institution, as well as more effective communication between public bodies.

3. I've been thinking: is access to information really a human right?

Yes! The right of access to information is a fundamental, universal human right.

And it's not just us saying this: there are plenty of decisions by national and inter-

national courts confirming that access to information is a human right. In the **OSCE region** 45 of the 56 participating states now have specific access to information laws (those that don't are: Andorra, Belarus, Cyprus, the Holy See, Kazakhstan, Luxembourg, Malta, Monaco, San Marino, Spain, and Turkmenistan). In addition a total of 25 European

constitutions recognise some kind of right of access to official documents or information and a total of 35 include the right either of access to information or "freedom of information". The **European Union** has a set of rules on access to EU documents and, after the adoption of the "Treaty of Lisbon", the **Treaty on the Functioning of the European Union** also establishes a right of access to EU documents.

In 2009 the **European Court of Human Rights** also recognised that there is a fundamental right of access to information held by public bodies protected by Article 10 of the Convention, which is the article on freedom of expression: *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.*

The Court said that the right to information is especially protected when these bodies are the only ones who hold this information (an "information monopoly") and when the information is needed by media or by civil society organisations who are using the information to facilitate public debate and to hold governments accountable.

The European Court rulings echoed a 2006 decision by the **Inter-American**

Court of Human Rights which confirmed that the American Human Rights Convention (Article 13) protects the "right of all individuals to request access to State-held information ..." and that there is a "right of the individual to receive such information and the positive obligation of the State to provide it ..."

This is exciting news for journalists: it is now clearly established that the right to freedom of expression, which includes the right to media freedom, is directly linked to the right of access to information held by public bodies. This means that any journalist who is requesting information from a public body has a right to that information linked to international protection for media freedom.

If you are interested in the human rights treaties, check out the following :

- Universal Declarations of Human Rights - Article 19
- International Covenant on Civil and Political Rights (ICCPR) - Article 19
- American Convention on Human Rights - Article 13
- European Convention on Human Rights - Article 10
- Declaration of Principles on Freedom of Expression in Africa - Article IV

See www.access-info.org for more details.

It does not mean that journalists have a stronger right than other citizens – freedom of expression is a right of everyone, of course – but it does make a very strong legal case when you need to go to court to defend any refusals to provide you with information.

The right to information is also recognized in many international and regional treaties and conventions on human rights. In the majority of cases it is recognized within the right to freedom of expression, which includes the right to seek, receive and impart information and ideas.

Constitutions that guarantee the right to know: In addition, many countries have recognized the right to information or access to administrative documents in their constitutions, either within the right to freedom of expression or separately as a stand-alone right of access to documents or access to information. At least 51 countries around the world have Constitutions which make this clear.



Have you ever read your country's constitution? If you want to know more, visit the website www.Right2INFO.org. There's lots of legal stuff there and you can find extracts from Constitutions from around the world.

Examples of the provisions on access to information in some European constitutions can be found in Box B.

TIP! Go to www.Right2INFO.org to check the language of your national constitution and see whether it gives you a right of access to information, or at least mentions “freedom of information” or “freedom of expression”. Knowing this can be useful if you are trying to persuade a public official that you know your rights and are ready to defend them in order to get the information you are looking for.

4. Who has the right to submit information requests?

The right of access to information is a fundamental right and therefore it's a right of everyone, no matter which country they live in. Almost all national access to information laws recognise this and state that “anyone” may submit an access to information request.

Furthermore, in many countries, the only formalities for submitting a request are a name and either a postal or an e-mail address, so the request process is open to everyone. One notable exception among the worlds' largest democracies is Canada where only citizens and residents may submit requests.

For requests submitted to the European Union, anyone may submit a request

but only citizens, residents, and businesses registered inside the Union have the right to appeal to the Ombudsman. Other requesters have to appeal to the Court of First Instance, which is a more complex procedure requiring the assistance of a lawyer.

In practice, however, a major obstacle to the transnational exercise of the right of access to information is that requests normally have to be submitted in the **official language(s)** of the country. Very few countries accept access to information requests in languages other than official languages. An exception is Sweden with its long tradition of transparency. The Swedish Administrative Act, Section 8 requires that “*When an authority is dealing with someone who does not have a command of the Swedish language or who has a severe hearing impairment or speech impediment, the authority should use an interpreter when needed.*” The Ministry of Justice reports that they quite often receive applications written in English for access to documents and that this has never constituted a problem.

Another example of a country which is ready to receive information requests in English is Slovakia, which has a contact form on its website for submitting access to information requests in English.

In general however, it's advisable to find a journalist or NGO in the country who

can help you submit your request. The **Legal Leaks Network** will help with this by providing you with contact persons in other countries.



The **Legal Leaks Network** is a network of journalists who are using the access to information laws in their countries and other countries for their research.

The aim of the Legal Leaks Network is to put these journalists in touch with one another and to provide **mutual support** filing requests in each others' countries.

The Legal Leaks team will also put journalists in touch with experts on access to information in their country and in other countries, including lawyers who can give advice about filing appeals.

The Legal Leaks website also has a section with **case studies** on the of stories written following filing of access to information requests. These can be stories based on the information you obtained or on refusals. If you have good stories to share with other journalists, please do let us know.

If you want to participate in the Legal Leaks network, you can sign up at www.LegalLeaks.info.

BOX B:
National and International Right to Info Guarantees

Many countries have recognized the right to information or access to documents in their constitutions, either within the right to freedom of expression or separately as a stand-alone right of access to information/documents. At least 50 countries around the world have Constitutions which make this clear.

Treaty on the Functioning of the European Union (Treaty of Lisbon)

Any citizen of the Union, and any natural or legal person residing or having its registered office in a Member State, shall have a right of access to documents of the Union institutions, bodies, offices and agencies, whatever their medium, subject to the principles and the conditions to be defined in accordance with this paragraph.

In Finland, Section 12(2) of the Constitution (2000) states:

Documents and recordings in the possession of the authorities are public, unless their publication has for compelling reasons been specifically restricted by an Act. Everyone has the right of access to public documents and recordings.

Similarly in Norway, the Constitution states at Article 100:

Everyone has a right of access to the documents of the State and of the municipal administration and a right to be present at sittings of the courts and elected assemblies. The law may prescribe limitations to this right in regard to the right to privacy or other weighty considerations.

Poland at Article 61 of the 1997 Constitution states:

A citizen shall have the right to obtain information on the activities of organs of public authority as well as persons discharging public functions.

Soon after the fall of Communism, Romania enshrined the Right to Information in Article 31 of the 1991 Constitution

- A person’s right of access to any information of public interest shall not be restricted.
- The public authorities, according to their competence, shall be bound to provide correct information to the citizens in public affairs and matters of personal interest.

5. Which information or documents does the right apply to?

In principle, all information held in a recorded form by public authorities can be accessed under access to information laws, unless there is a strong reason to refuse access (See Point 8 below on exceptions).

Some laws refer to “access to information” and others to “access to documents”. Normally the definitions overlap and both are very wide concepts and include many kinds of formats on which information is held (including photographs, videos, DVDs, etc.) In practice there

is little difference, but it is useful to know what the law says so that you can formulate your request in a way that is most likely to result in an answer.

The new Council of Europe Convention on Access to Official Documents defines “official documents” as “all information recorded in any form, drawn up or received and held by public authorities” (Article 1.2.b).

The EU Regulation 1049/2001 defines “document” as “any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audiovisual recording) concerning a

BOX C:
Access to Information or Documents?

Access to Documents	Access to Information	Both Documents and Information
European Union, Belgium, Denmark, France, Greece, Italy, Kosova, Liechtenstein, Sweden, Switzerland, Canada, USA.	Armenia, Austria, Azerbaijan, Bosnia & Herzegovina, Bulgaria, Croatia, Czech Republic, Estonia, Georgia, Germany, Hungary, Kyrgyzstan, Latvia, Moldova, Montenegro, Romania, Serbia, Slovakia, Slovenia, Tajikistan, Ukraine, Uzbekistan, United Kingdom.	Albania, Finland, Iceland, Ireland, Lithuania, Macedonia, Netherlands, Norway, Poland, Portugal, Russia, Turkey.

matter relating to the policies, activities and decisions falling within the institution's sphere of responsibility" and this applies to "to all documents held by an institution, that is to say, documents drawn up or received by it and in its possession, in all areas of activity of the European Union."

Note: Requests to the EU should specifically mention "documents" or they may be processed under the Code of Good Administrative Procedure which refers to the "right to information" but does not have the same timelines nor appeals possibilities.

Note: It is important to know if your law is an access to documents or access to information law because this can affect how you formulate the question – more advice about this is given in Section I.

6. What about access to an entire database?

The right of access to information clearly applies to all documents and to other materials stored in other formats, such as audio-visual materials stored on tapes, CDs or DVDs.

A question arises when it comes to access to information stored in databases. This issue is very important for journalists who may want to get at more detailed information rather than a simple answer to a question.

In general, public authorities are not required to generate new documents or information in response to requests. They normally will be ready to extract some information from a database using a simple search. This is something which is required following decisions of the Information Commissioners in countries such as France and Slovenia.

In some countries, a database is considered to be a "document"; in other countries a document is limited to a coherent set of information which can be extracted from a database. Access to information and open government data campaigns are now arguing that access should be granted to entire databases, not just the information contained in them. In the meantime, this is something which **journalists** should be aware of and check the situation in your country if you are planning to ask for an entire database.

At the same time, something very exciting is happening to government databases which should be of interest to all journalists: the "Open Government Data Revolution" in which public institutions are releasing entire databases to the public by putting them on line in central web portals. See Box D on Open Government Data. Good training in **Computer Assisted Reporting Techniques** is now essential in order to make the most of these new information resources.

BOX D: Open Government Data

What is open government data?

The release of databases and other collections of information by government departments in formats that can be freely used, reused and distributed. Release is generally proactive, without the need for access to information requests.

What are governments doing to promote access to datasets?

There are currently a number of initiatives to release government data in bulk, these include:

- **United States:** On 21 May 2009 the US Government launched Data.gov whose purpose is to give direct public access to machine-readable datasets generated by the Executive Branch of the US Federal Government.
- **United Kingdom:** Working with Tim Berners-Lee, one of the inventors of the World Wide Web, the UK government has created Data.gov.uk, a single online access point for government data, launched on 21 January 2010
- **Australia:** the data.australia.gov.au website links to numerous databases and encourages users to "make government information even more useful by mashing-up the data to create something new and exciting!"
- **New Zealand:** Recent releases on data.govt.nz include a database from the food safety authority with a breakdown of the major causes of food recalls, and the total number of recalls from 200 to 2009, as well as hospital performance data from the Ministry of Health.
- **Denmark:** The Danish National IT and Telecom Agency has created a meta-portal to link, Digitaliser.dk, to guide users to available public data

What are other issues for journalists to be aware of?

There are potential obstacles to accessing full government data, such as that information released in formats that can't be read by computers is difficult to reuse or the data or database itself is subject to copyright or other licences. Another obstacle is that data is released under a reuse licences for which users have to pay

These problems are still being resolved by open government data activists in discussions with governments. In the meantime, where governments have released data, such as on the portals listed above, journalists might want to start surfing through, while thinking creatively about what stories it might generate.

7. Does the right apply to all public bodies?

In Europe the right of access to information is firmly established as applying to all **administrative bodies**, at the central, regional and local level. There are rare exceptions to this – in Ireland the police force is exempted for example.

In addition, as the right has developed, it has been progressively applied to **legislative and judicial bodies**. Almost all countries grant access to administrative information held by legislative and judicial bodies, and most grant access to all information held by legislative bodies.

In many countries **private bodies performing public functions or operating with public funds** also have the obligation to respond to requests for information.

For example, in Macedonia, one of the last countries to adopt an ATI law (2006), the right of access encompasses the government at national and local level, legislative bodies and judicial authorities, and private bodies (natural and legal persons) that perform public functions and all other bodies and institutions that are established by law.

There are however exceptions – the Norwegian parliament for example or court documents in a few countries – so it's important to check these before plan-

ning a request strategy. Annex C gives details.

TIP! Follow the money: *If the body you are interested in is not covered by the scope of the access to information law in your country, then think if it has to report to another body. For example, some private bodies which operate with public funds have to submit reports to the ministry which is providing the funding. So use the principle of follow the money and ask for those reports.*

8. What about inter-governmental organizations?

Many inter-governmental bodies hold information about decisions which affect our lives. These include the European Union, the World Bank, the Inter-American Development Bank, the African Development Bank Group, the Asian Development Bank, the European Bank for Reconstruction and Development and the United Nations Development Programme.

The EU has access to documents rules but there is still a lot of discussion about whether the right of access to information applies to intergovernmental organizations because they are outside the scope of national laws and also do not sign international human rights treaties. Thanks to the work of campaigning groups such as the **Global Transparency Initiative**, many of the key inter-

governmental organizations that are active in the aid world do have internal rules which are a bit like national access to information laws. These are called “disclosure policies” or “access to information policies”. For example, the World Bank’s new Access to Information Policy which came into force on 1 July 2010.

9. But can I get access to all information held by public bodies?

No. The right of access to information is **not an absolute right**. There may be some small quantities of information that public bodies hold that would cause harm if they were released, at least if released at this point in time. So although the right

applies in principle to all information, in fact there are **exceptions**.

For example, to release all information about an ongoing police criminal inquiry might harm the possibility of catching the suspect. After the criminal is arrested, the information can be released without it causing any harm.

This is an example of information being withheld to protect what is known as a “legitimate interest”. To justify withholding information public bodies must demonstrate that there would be harm to a predefined interest specified by law. Exceptions permitted by international law include:

Exceptions to protect state interests:

- Protection of national security and defence of the state
- Protection of international relations
- Protection of public safety or public order
- Protection of the economic, monetary and exchange rate policies of the state

Protections aimed at ensuring effective government:

- Protection of internal deliberations within public authorities prior to decision-making – this is known as the “space to think” exception
- Protection of criminal investigations

Exceptions to protect private interests and human rights:

- Protection of privacy and other legitimate private interests
- Protection of commercial and other economic interests, such as protecting trades secrets or the ability of a private company to compete effectively in the marketplace
- Protection of the environment [such as locations of endangered species]
- Guaranteeing the equality of parties in court proceedings or the effective administration of Justice

Wow! All these reasons? This seems like a long list, and can be a bit off-putting, but if properly applied, only a small percentage of all the information held by public bodies should be exempted from disclosure.

Even when a document contains some sensitive information, some or all of it may still be released because the public body has to consider two other key factors which are detailed below:

(i) Partial Access or “Give me the non-sensitive stuff”

Even if an exception applies, that doesn't mean you can't get any information. In most countries, public bodies are obliged to black out or otherwise remove the sensitive information and give you the rest of the document. If the information is in electronic form, then the sensitive information can be removed electronically, but in that case the public body should tell you that they have done some “editing” and mark where that was and they should justify in detail why it was necessary.

The right to have partial access to documents is part of the right to information because it's a right to know all non-sensitive information. This is a right projected by the Council of Europe Convention on Access to

Official Documents and national and international jurisprudence.

For **journalists**, even partial access to information can be useful for two reasons. First, you can make use of the information you get and you can write a story about what the government is not giving you. Second, you can use the information you have received to make a follow-up request for the remaining information or you can use it in an appeal to an Information Commissioner or the Courts (see Point 9 on Appeals).

(ii) Exceptions to Exceptions: When Transparency Trumps Secrecy

Sometimes information may be a bit sensitive but it is really important to make it public so that we know how the government is working or how our taxes are being spent.

For example, information about a contract between a public body and a private contractor will contain information about the money paid for the services of that contractor. If the contractor offered the government a very low price for its services, they might not want to disclose that information as it would hurt their ability to negotiate a higher price with other clients in the future. But on the other hand, the public has a right to know how public funds are being spent,

and there is a strong public interest in knowing that the taxpayer's money is being used properly, so the information should be disclosed.

In this kind of example, public officials have to apply what is called the “public interest test”. They have to consider the exceptions, and the possibility of not releasing the information, and then they have to consider the public's interest in knowing the information. Many access to information laws have this kind of test built into them. In other cases the Information Commissioner or Courts will consider the public interest when there is an appeal.

In a well functioning access to information regime, there will be many cases when transparency overrides secrecy.

Note: What about copyright problems if I reuse or publish the information? Copyright and rules on reuse of public sector information are important issues which journalists need to be aware of. Generally if information is released from public authorities under freedom of information laws, it may be reused by the media for stories and radio and TV programmes and for posting on blogs. Because of the importance of freedom of expression, in some countries this is considered to be “fair use” of the material and not subject to copyright or reuse

licences. You need to check the rules in your country. Also, if you plan to make use of a large volume of information such as an entire database, then you may need to check with the public institution about the rules on reuse.

10. Appeals against silence and refusals

If your request is not answered (“administrative silence”), or if the public institution refuses to provide you with the information, or if the answer doesn't really answer your question, you may want to appeal. The rules for appealing vary from country to country. Annex D has a list of the 45 countries in the OSCE region which have access to information rules and summarises the appeals procedure as well as giving links to the relevant oversight bodies. It is advisable to check the rules and timeframes for appealing in your country before you submit a request or as soon as you have submitted it. That way you will know when to expect a response and you will be ready to present the relevant appeal.

There are four main appeals mechanisms:

» **Internal or Administrative Appeal:** this is an appeal to the same body which issued the denial or to the immediately superior administrative body. It may seem strange to appeal to the same body, but it signals to them that you are serious about defending your

right and can often result in a change of mind. In any case, in most countries the request for internal review is required before submitting an appeal to the Information Commissioner, Ombudsman, or Courts. Sometimes however, an appeal may be made directly to the Information Commissioner or Ombudsman. Box D lists these options.

» **Administrative Court Appeal:** in many countries, particularly those without an Information Commission or Ombudsman responsible for overseeing the access to information law, the next step is an appeal to the courts. Normally access to information appeals are regulated by administrative law, and so appeals should be made to the regional or national administrative court, with a further appeal to a higher court usually possible. In 11 Council of Europe countries court appeals are the only option.

» **Information Commission/er:**

these are specialised bodies whose role is to defend the public's right to know. Often the body is combined with that of a data protection oversight body. 13 Council of Europe countries have a specialised oversight body. Some can issue binding decisions, others can only make recommendations. In some countries, the decisions of the Information Commissioners can be appealed to the courts.

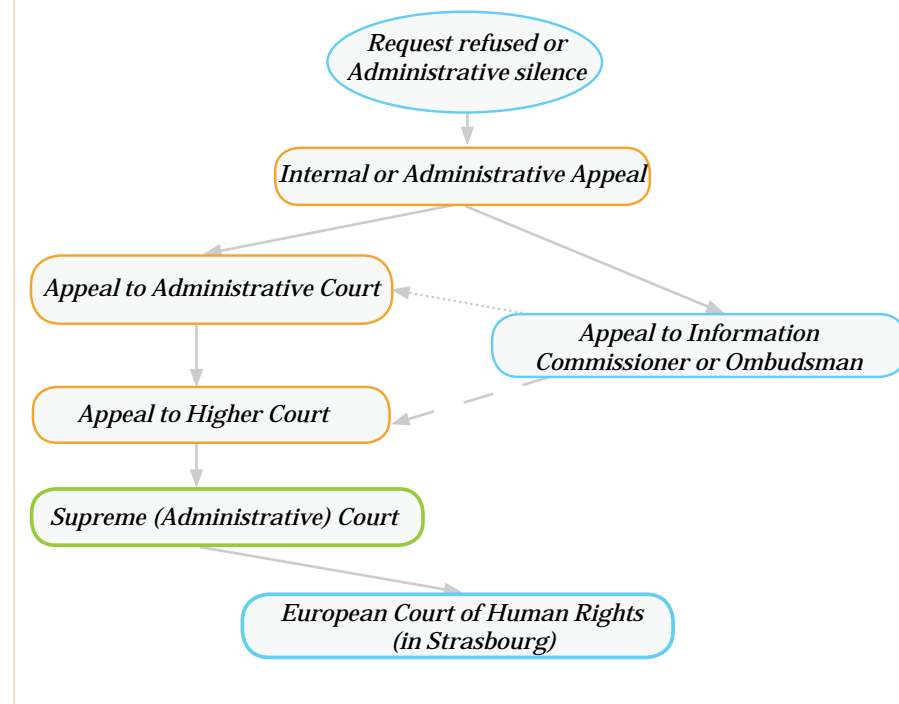
» **Ombudsman:** In many countries the Ombudsman plays the role of protecting the rights of citizens and residents in their interactions with public bodies. In 13 of these countries, the Ombudsman also has the role of receiving complaints related to the access to information requests. Often the Ombudsman's Office can only issue recommendations although their power to criticise means that in many countries the public authorities will comply with these recommendations. At the EU level as well, the European Ombudsman will process complaints related to access to documents requests.

BOX E: Appeals mechanism in the Council of Europe region

Court Appeal	Information Commission/er	Ombudsman
Bulgaria, Czech Republic, Georgia, Latvia, Liechtenstein, Moldova, Netherlands, Poland, Romania, Russia, Slovakia, Ukraine	Belgium, Canada, France, Germany, Iceland, Ireland, Italy, Macedonia, Portugal, Serbia, Slovenia, Switzerland, Turkey, United Kingdom	European Union, Albania, Armenia, Austria, Bosnia, Croatia, Denmark, Estonia, Finland, Greece, Kosovo, Lithuania, Norway, Sweden

Figure 2: Appeals Process step-by-step

In most countries there are two or three steps to the appeals process:



Presenting internal administrative appeals is normally quite easy and free of charge (there are exceptions such as Ireland where it costs €75 which is a huge disincentive to defending your right to know!). Sometimes it helps, however, to have the advice of a lawyer or specialist organisation. If in doubt, contact the **Legal Leaks Team** and we will try to put you in touch with someone in your country who can help you.

Appeals to higher courts and to the European Court of Human Rights can take a long time (even years!) but are well worth considering for two reasons:

» **Good deed**, legal challenges contribute to the long term development of the right of access to information;

» **Good story: launching an appeal makes a good story** and can have immediate political impact even though you are still waiting for the formal legal decision!

III. DATA SECURITY FOR JOURNALISTS

1. Risk Assessment: How do I conduct an assessment of my security risks?

Could you provide me with a flow chart that I can use to do this? I need solutions that are not too geeky or complicated and I just need to be told what I should do, not to be given options because I am a busy journalist and don't have time to think.

» **What is the threat?** You probably already know what the level of threat is and where it is coming from. Depending on the nature of your work, the vulnerabilities may be public authorities, criminals, foreign governments or others.

» **What information is at risk?** Divide the information you have into three categories: confidential, personal, and public. Remember to think of all the information you hold when doing this, including paper files, computer documents, e-mails, contact information, text messages, and other data, even scraps of paper with names and telephone numbers written on them. The “confidential” category should include the information that is most sensitive and really needs protection. Start there.

» **How is the information stored?** The different storage systems which

you use will result in different levels of risk. Make a list of where your sensitive or “confidential” information is stored: computer hard drives, e-mail and web servers, USB memory sticks, external USB hard drives, CDs and DVDs, mobile phones, printed paper and hand-written notes. Think about the physical locations as well: Is information kept in the office, at home, in a trash bin, or “somewhere on the Internet”?

» **How is information communicated?** Think how you typically communicate: paper letters, faxes, landline phones, mobile phones, e-mails and Skype messages. You will need to have this information as your read about the potential vulnerabilities in the questions below.

A basic starter level data security scheme for your confidential information:

i) **Encrypt** the confidential information (How-to, more info on encrypting: see Q3,Q5)

ii) **Protect**: Physically prevent access to files and folders (printouts and other physical representations of data)

iii) **Destroy** unwanted information (shredding, destroying data). Note that simply deleting a file doesn't actually erase the information, and leaves the data

somewhere on the storage device to be overwritten (or recaptured). In order to completely remove the data, you need to use a specific tools such as CCleaner (see http://security.ngoinabox.org/en/ccleaner_main).

2. I'm afraid that my notebook computer will get stolen.

I really can't afford to lose my research data, so I would prefer to store it online. Is this safe to do? Where can I store data safely?

Option 1: Put your sensitive data on the internet or “in the cloud”. An example of a service is Dropbox, which offers free storage of 2GB of data and for about €8 a month you get 50GB. Some commercial companies guarantee that data will be stored on several computers and/or encrypted, but you have to be ready to trust that the private company will not turn over the data.

Option 2: Use TrueCrypt, which allows you to keep your files in a “vault”, hidden somewhere on your file system. You can follow the steps for this at http://www.security.ngoinabox.org/en/truecrypt_main.

Option 3: Combine Options 1 and 2: Create a True-Crypt “volume”, and then upload it to Dropbox. This way, you are off-shoring your data to the cloud, AND it is pre-encrypted so if it is compromised by the service provider, the information is still unavailable to others.

3. Which is the safest form of telephonic communication?

I need to make phone calls with a source, but I am worried that someone will secretly listen to the conversation. What should I do?

Use Skype: Generally use of Skype is safer, so conduct Skype to Skype conversations wherever possible.

Is it true that Skype is secure and that the traffic data is not retained? According to Skype, data transfers are encrypted, but they are retained. If true, this may mean that the content of the data transfer may not be exposed, but a record of a transaction would still exist.

Note: Skype calls to fixed or mobile phones fall into the domain of phone networks, which are typically NOT encrypted. You should also be aware that in some countries Skype is less secure. This is the case in China for examples for users of TOM-Skype which is Skype's distribution inside China.

For very sensitive communications use a Skype account with a nickname that is only for communicating with that contact. Do not put credit into this account so that your bank or credit card info will not be associated with it.

4. Using mobile phones: How risky is it to use a mobile phone?

» **Make your phone harder to use**

if lost or stolen: Activate your mobile phone's password or pin lock so that if it is stolen it cannot be easily accessed. Regularly delete unwanted and/or sensitive information on your phone. If you use your phone, don't save sensitive information on it, or if you have to, obfuscate it so only you can understand it.

Dedicated phones for single sources: When working with individuals and organisations transmitting sensitive information, you should consider having separate phones and SIMs for different uses, and maybe a temporary anonymous phone number that you only use for contact with a particular source.

» **Mobile phones can be tapped and tracked.** Even if they seem to you to be switched off. You may not be aware of this as it only takes seconds to set a phone so that it can be tracked. Be continually aware of your environment when bringing out and using your mobile phone, and refrain from this in risk prone places and situations.

» **Disable your cell phone's Bluetooth connection.** This will prevent any signals being sent to or from your phone. If needed, contact your carrier for disabling instructions. Read more: How to Stop Phone Tapping | eHow.com http://www.ehow.com/how_7443526_stop-phone-tapping.html#ixzz1FGPUMM5e.

» **Use voice encryption software on your phone.** There are paid services available on some but not all mobile phones. The encryption software will

need to be installed on both phones for communication to be secure. An example is <http://www.cellcrypt.com/>. Software is in development for android phones to encrypt transmission; again, both ends of the conversation would need to have encryption.

TIP! Think carefully before using mobile phones to send sensitive information; if possible use a more secure alternative.

5. Security using e-mail accounts *I want to communicate with a confidential source, should I use my normal e-mail to contact them or do anything differently?*

It is always a good idea to use different communications channels when transmitting sensitive information. In this case it is recommended that both you and the contact use different e-mail addresses from the ones you normally use – it doesn't make sense to secure only one side of the communication channel!

Make sure that both of you create an e-mail address that is not traceable by registering it with another name and address, a pseudonym.

If possible encrypt the contents of your e-mail messages. Both you and your source should be using encryption. One solution is to use VaultletSuite a secure and encrypted e-mail service. Please refer to http://security.ngoinabox.org/en/vaultletsuite_main for installation and use.

6. Remembering Passwords

I have too many accounts that I need passwords for. In order to remember them I sometimes use the same passwords and often they're not very secure. Is there a way to manage my passwords?

» **Don't write your passwords down** in a way that makes it easy for someone to access all your accounts if they find the piece of paper!

It is always a good idea to have longer and more complex passwords and at the same time have different passwords for each service/account on the internet. The ideal solution is to use a password manager that allows you to store passwords securely and also allows you to generate more complex passwords automatically.

» **Use a password manager:** When using a password manager you only need to remember one (1) secure password. A master password then unlocks your password manager so you will have access to your other passwords. Please refer to http://security.ngoinabox.org/en/keepass_main for details on how to use keepass, a secure and encrypted password manager.

7. How to I protect the security of my normal e-mail account?

E-mail remains the main communication medium on the internet, widely used for personal and/or work purposes. You

need to ensure security at each stage of the journey that an email takes. Think of it as a package you are posting: are the contents fragile? Is it well packed? Are you sending it via a reliable company? Are there dangers on the road? Will there be someone at the other end to receive the package?

Security at every stage is essential:

» **Security of Content:** Ultimately, it is your content that you are trying to keep from being exposed. You can encrypt your e-mail content and send it to the recipient. Many e-mail applications can be configured to encrypt the content of your e-mails, for which you (as well as your communication partners) will have to take additional steps. Read more about how to encrypt your e-mails at: http://security.ngoinabox.org/en/chapter_7_4.

TIP! You should also think twice before setting "pen to paper" or hitting the keyboard and pressing the send button: could the message be phrased in a way that will make your source and your story less vulnerable if it did get into the wrong hands?

» **Interface Security:** Instead of Outlook, use a mail client application such as Thunderbird or VaultletSoft, which provide increasing security measures. If you have to access your e-mail via the web, use a browser such as Firefox, as it has fewer security vulnerabilities, and has the capability to be augmented with security measures. See Security-in-a-Box for

more details.

» **E-mail Provider Security:** Your information (e-mails, attachments, etc) is located on your e-mail provider's servers. You have little say about how these are operated: you trust the service providers with your information and that of those who communicate with you. If your data security is important, you should understand how the service provider treats your information and read the privacy policy and other legal agreements before clicking an "I agree" button. If your organisation has its own server, your IT department may be able to set up a main e-mail account and additional accounts for you. They will tell you how secure these e-mails are both when being accessed inside the office and when being accessed when out of the office.

For more sensitive e-mails and communication please consider using free e-mail services that explicitly say they will secure and not use/divulge your information. Read more here http://security.ngoinabox.org/en/riseup_main. Use dedicated e-mail accounts for communicating with a single source.

TIP! You and your source can access the same Gmail account and create and save draft messages. This helps increase security by not sending the messages over the internet.

» **Transmission Security:** Make sure your e-mails are travelling through the Transport Layer Security ("TLS" or its predecessor "SSL") which is a commu-

nications protocol with enhanced security. Check if your e-mail provider offers this. When using e-mail in a browser, check the address bar in the browser: if the address starts with "http", then your transmission is NOT secure; if it starts with "https", then it is secure. Currently Gmail provides https or secure transmission of all e-mail correspondences to and from its servers.

Note: Communication is a two-way process. Make sure that the person you communicate with also uses a secure service. It does not make your e-mails secure if only one party uses a secure service. Your security is as weak as the weakest link.

7. How should I store and back up my data? *How can I make sure that my data is stored in a way that means that I never have to worry about losing it and that nobody else can access it?*

» **Good physical security:** Protecting computers should not only be restricted to the data and information inside your computers. It is always a good idea to look at physical security as well. This means putting in place policies that would restrict physical access to your office computers and ensuring that only authorised persons can enter.

It is helpful to place computers in more secure locations within the office premises. Having these located in restricted

areas may help unwanted access and usage. This can only protect to a certain extent, and a determined adversary can and will get access to your computers and your information.

» **Backups:** In addition to physical security having backups is a must. Having off-site backups is also a good idea and helps in cases where computers are physically damaged and inaccessible. You can have online offsite backups as well.

» **Avoid copying of your data:** Another threat to your data/information is the kind of theft you don't even know about because, being digital, information can be copied or transmitted elsewhere but still also remain on your computer. There may also be an attempt to tamper with your data by hacking into your computer and changing some important statistics, for example. One solution to data theft and tampering could be encryption which has been discussed in question 2.

» **Housekeeping:** One of the major causes of data loss remains accidental loss because a hard drive crashes or a virus of some kind gets into the computer. Regular upkeep of your computers is a must. This means regular update of anti-virus, operating system and application software. Have an IT expert check that the computer is running correctly. Bear in mind that a lot of insecurities come via your internet connection, capitalising on software and system vulnerabilities.

» **Useful resources on protecting data:** Protection from malware and hac-

kens - <http://security.ngoinabox.org/en/chapter-1> Protection of information from physical threats - <http://security.ngoinabox.org/en/chapter-2> Protection of sensitive files on your computer - <http://security.ngoinabox.org/en/chapter-4>

8. What is your advice for online tools? *I have created a Google map - just how private is this? How can I protect it better?*

According to Google, you have a choice to make a private or a public Google map. The extent to which this assertion can be explored, or for that matter, what private means in this case, is unclear. In general, using online tools should be preceded by considering the following issues:

Data ownership: Using online tools exposes your information to the owner of the site of the tool. In all cases, the extent of the exposure of your information is spelled out in legalistic terms in the EULAs of these tools. It is imperative to read and understand the scope of what you relinquish in terms of data ownership with these tools.

Data association: In many cases, these tools are connected to an online profile (such as an e-mail account on Google, or a Facebook account). Usage of such tools then connects the data you are uploading/sharing on these tools with these online identities. In some cases, this may be inappropriate, incriminating, or dangerous.

Data transfer: It is also important to determine how the data is transferred as part of using and sharing these tools, especially if the information being kept is confidential.

9. What about the borders between my professional and private life? *I am a journalist who travels a lot and makes friends with the people I meet. Some of those are also sources. Is it safe to communicate with them by Facebook and similar social networking sites?*

You can keep your privacy settings turned up high on Facebook but be aware that the information is considered to have been shared with Facebook and that they therefore have access to it. A court could order this information to be handed over. You therefore need to be very discerning about what you post and assume that it might be accessed. If someone would be seriously compromised by the fact that they know you being revealed, then consider using other means to communicate with them.

The same applies to Twitter: although all the communication is in the public domain, the background information such as which IP address messages were sent from is held by Twitter and a court could try to get hold of this information.

» **Is it possible to create web pages/blogs/some online space**

where I can put information that interests me personally, but which is totally private and/or accessible to only a few people who have the password?

This is possible and some online services provide this configuration. Below are a couple of links on how to configure these:
<http://www.google.com/support/blogger/bin/answer.py?hl=en&answer=42673>
<https://en.support.wordpress.com/settings/privacy-settings/>

10. Caught on Camera *Should I worry about being recorded on CCTV cameras in public?*

Invasion of privacy and the misuse of the recordings are the primary concerns in regards to the use and implementation of CCTVs. If you are meeting a secret source, make sure to do so in a place which is less likely to have CCTV cameras. These days underground car parks are about the worst places to meet your “deep throat” as they are full of cameras!

11. I travel a lot, should I change my behaviour depending on where I am? *In what regions of the world, or in what types of places should I be most careful regarding the security of my data?*

It is always a good idea to **get information in advance** about the places you

will visit and to adjust your behaviour accordingly. This is not only about your safety but the safety of the people in those countries who help you and the safety of the people you interview. Threats may come for political reasons or because you are investigating criminals – or both.

There are some things which you can always do when travelling, no matter where you are going, just to be on the safe side:

» **Before travelling, make a backup of all your data and information.** Store the information somewhere safe back at home as well as online if you will need to access it while travelling.

» **If you are have sensitive data, seriously consider either leaving it behind** or encrypting what you carry with you. Only carry what is absolutely necessary.

» **Be especially careful when accessing the internet in public spaces.** Even when on a Wi-Fi network that requires a password (such as the hotel you are staying in) remember that someone in a neighbouring building may have the password and have hacked the network – they may do this to get sensitive data or just to access your bank account when you go online to make a payment. Try to do all banking and password protected operations when at home.

» **Physically secure your laptops and mobile phones when travelling, or in other countries.** Even in the internet age, most data is still lost

due to computer theft. If you are attending a conference, consider a lock such as Kensington lock if you are going to leave your computer on a table while going to a coffee break.

» **Be extra careful in communicating with sources** and make sure you take all the steps in the previous sections when making contact with sources. Take care also to hide the identity of people you have interviewed – in your computer and in your notebook – especially if you have promised to keep their names anonymous.

TIP! Before travelling, check the following links for country-specific profiles relating to internet and information restrictions:

<http://advocacy.globalvoicesonline.org/projects/maps/>
<http://opennet.net/accessdenied/>
<http://www.access-controlled.net/>

ANNEX A:**Adoption of Access to Information Laws 1766-2010**

Year	Countries*	No. of Laws Adopted	Total
1766-1950	Sweden	1	1
1951-1960	Finland	1	2
1961-1970	United States	1	3
1971-1980	Denmark, Norway, France, Netherlands	4	7
1981-1990	Australia, Canada, New Zealand, Colombia, Greece, Austria, Italy	7	14
1991-2000	Hungary, Ukraine, Portugal, Belgium, Belize, Iceland, Lithuania, South Korea, Ireland, Thailand, Israel, Latvia, Albania, Portugal, Czech Republic, Georgia, Greece, Japan, Liechtenstein, Trinidad & Tobago, Bulgaria, Estonia, Moldova, Slova- kia, South Africa, United Kingdom	26	40
2001-2010	Bosnia & Herzegovina, Poland, Romania, Serbia, Jamaica, Angola, Mexico, Pakistan, Panama, Peru, Uzbekistan, Tajikistan, Zimbabwe, Armenia, Croatia, Kosovo*, Slovenia, Turkey, St. Vincent & Grenadines, Dominican Republic, Ecuador, Switzer- land, Antigua & Barbuda, Azerbaijan, Germany, India, Montenegro, Taiwan, Uganda, Honduras, Macedonia, Jor- dan, Kyrgyzstan, Nepal, Nicaragua, China, Chile, Cook Islands, Uruguay, Indonesia, Bangladesh, Russia	42	82

*Kosovo is the only non-UN, non-OSCE member country in this list; it is recognised by 65 UN Members, including 22 of 27 EU Countries and the United States.

ANNEX B:**Access to Information Laws in the 56 OSCE Participating States**

Country	Name of the Act	Year
Albania	Law on the Right to Information over the Official Documents	1999
Armenia	Law on Freedom of Information	2003
Austria	Duty to Grant Information Act	1987
Azerbaijan	Law Of The Repbluic Of Azerbaijan On Right To Obtain Information	2005
Belgium	Belgian Constitution (See Article 32) Law on the right of access to administrative documents	1994
Bosnia and Herzegovina	Freedom of Access to Information Act	2000
Bulgaria	Access to Public Information Act	2000
Canada	Access to Information Act	1985
Croatia	Act on the Right of Access to Information	2003
Czech Republic	Law on Free Access to Information	1999
Denmark	Access to Public Administration Files Act (No. 572 of 1985)	1985
Estonia	Public Information Act	2000
Finland	Act on the Openness of Government Activities	1999
France	The Right of Access to Administrative Documents	1978
Georgia	Law of Georgia "On Freedom of Information" – The General Administrative Code of Georgia (See Chapter 3)	1999

Country	Name of the Act	Year
Germany	Federal Act Governing Access to Information held by the Federal Government - (Freedom of Information Act)	2005
Greece	Code of Administrative Procedure	1999
Hungary	Act LXIII OF 1992 on the Protection of Personal Data and the Publicity of Data of Public Interest	1992
Iceland	Information Act (No. 50/1996)	1996
Ireland	Freedom of Information Act 21 April 1997, entered into force 21 April 1998	1997
Italy	New provisions on administrative procedure and right to access to administrative documents, Law 241/90	1990
Kosovo	Law on Access to Official Documents	2003
Kyrgyz Republic	Law on Access to Information held by State Bodies and Local Self-Government Bodies	2007
Latvia	Freedom of Information Law	1998
Liechtenstein	Information Act	1999
Lithuania	Law on Provision of Information to the Public (No. I-1418)	1996
Macedonia	Law on Free Access to Public Information	2006
Moldova	Law on Access to Information	2000
Montenegro	Law on Free Access to Information of Public Importance	2005
Netherlands	Act on Public Access to Government Information	1978
Norway	Freedom of Information Act (No.69, 1970)	1970

Country	Name of the Act	Year
Poland	Act on Access to Public Information	2001
Portugal	Law of Access to Administrative Documents	1993
Romania	Law Regarding the Free Access to the Information of Public Interest (No. 544)	2001
Russia	Law on Providing Access to Information on the Activities of State Bodies and Bodies of Local Self-Government	2009
Serbia	Law on Free Access to Information of Public Importance	2003
Slovakia	Act on Free Access to Information and Amendments of Certain Acts	2000
Slovenia	Act on the Access to Information of Public Character	2003
Sweden	Freedom of the Press Act	1766
Switzerland	Transparency Law	2004
Tajikistan	Law republic of Tajikistan on the right to access to information	
Turkey	Law on the Right to Information (No. 4982)	2003
Ukraine	Law on Public Access to Information	1992
UK	Freedom of Information Act	2000
United States	U.S. Department of State Freedom of Information Act (FOIA)	1966
Uzbekistan	Law on the Principles and Guarantees of Freedom of Information	2002

ANNEX C: The Scope of the Right of Access to Information

Country	Government and National Administration all levels	Legislative & Judicial – admin.info	Legislative Bodies, other info	Judicial Bodies, other info	Private bodies performing public functions
Albania	Yes	Yes	Yes	other info	public functions
Armenia	Yes	Yes	Yes	Yes	Yes
Azerbaijan	Yes	Yes	Yes	Yes	Yes
Belgium	Yes	Yes	No	Yes	Yes
Bosnia & Herzegovina	Yes	Yes	Yes	No	Yes
Bulgaria	Yes	Yes	Yes	Yes	Yes
Canada	Yes	Yes	Yes	Yes	Yes
Croatia	Yes	Yes	Yes	Yes	Yes
Czech Republic	Yes	Yes	Yes	Yes	Yes
Denmark	Yes	Yes	No	partial	Yes
France	Yes	Yes	No	No	Some
Georgia	Yes	Yes	yes	No	Yes
Germany	Yes	Yes	No	partial	Yes
Hungary	Yes	Yes	Yes	No	Yes
Ireland	Yes	Yes	Yes	partial	Yes
Kosovo	Yes	Yes	Yes	partial	Yes
Kyrgyz Republic	Yes	Yes	Yes		

Country	Government and National Administration all levels	Legislative & Judicial – admin.info	Legislative Bodies, other info	Judicial Bodies, other info	Private bodies performing public functions
Latvia	Yes	Yes	Yes	Yes	Yes
Macedonia	Yes	Yes	Yes	Yes	Yes
Moldova	Yes	Yes	Yes	Yes	Yes
Montenegro	Yes	Yes	Yes	Yes	Yes
Netherlands	Yes	Yes	Yes	Yes	Yes
Norway	Yes	Not parliament	No	Yes	Yes
Romania	Yes	Yes	Yes	Partial	Yes
Serbia	Yes	Yes	Yes	Yes	Yes
Slovakia	Yes	Yes	Yes	Yes	Yes
Slovenia	Yes	Yes	Yes	Partial	Yes
Sweden	Yes	Yes	Yes	Yes	Yes
Tajikistan	Yes			Yes	Yes
Turkey	Yes	Yes	No	No	Yes
United Kingdom	Yes	Yes	Yes.	No	Yes
United States	Yes	No	No	Partial	Yes
Uzbekistan	Yes			No	No

ANNEX D: Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
European Union	
FIRST Administrative appeal to the same body, called “confirmatory application” THEN Ombudsman OR Court of First Instance	<i>European Ombudsman</i>
Albania	
FIRST Administrative appeal THEN Judicial appeal OR complaint to Ombudsman	<i>People’s Advocate (Ombudsperson) – decisions are not binding</i>
Armenia	
FIRST Administrative appeal followed by appeal to the Courts (recommended) OR Ombudsperson	<i>Human Rights Defender of the Republic of Armenia (Ombudsperson) – decisions are not binding</i>
Austria	
FIRST Administrative appeal THEN Appeal to the Courts	<i>Austrian Ombudsman Board Volkanwaltschaft</i>
Azerbaijan	
FIRST Appeal to authorized agency on information matters. OR Appeal to Courts	<i>Authorized Agency on Information Matters</i>

Appeal Options, by Country	Oversight Body
Belgium	
Belgium FIRST Appeal to administrative body AND at same time Commission for Access to Administrative Documents for advisory opinion THEN application to Administrative Court for annulment of refusal to grant information	<i>Commission (fédérale) d'Accès aux Documents Administratifs</i>
Belgium – Flanders FIRST Application to the Appeal Instance for annulment of refusal to grant information THEN Application to Supreme Court for annulment of refusal to grant information	<i>Appeal Instance on access to administrative documents and the re-use of public sector information</i>
Belgium – French Community of Belgium FIRST Appeal to administrative body AND at same time Commission for Access to Administrative Documents for advisory opinion THEN Application to Supreme Administrative Court for annulment of refusal	<i>Commission d'Accès aux Documents Administratifs (specific to the French Community of Belgium)</i>
Bosnia Herzegovina	
FIRST Appeal to head of the public authority that issued the decision THEN apply for judicial review, OR complaint to Ombudsman	<i>Ombudsman for Human Rights</i>

Appeal Options, by Country	Oversight Body
Bulgaria	
FIRST Administrative Appeal OR (depending the body) Regional courts or Supreme Administrative Court	<i>No oversight body – appeal to courts</i>
Canada	
FIRST Complaint to Information Commissioner THEN Appeal to the courts	<i>Office of the Information Commissioner of Canada</i>
Croatia	
FIRST Administrative appeal to head of the administrative body THEN Administrative court OR Ombudsman	<i>Ombudsman</i>
Czech Republic	
FIRST Appeal to superior body of the public body that issued the decision THEN If the latter has rejected the appeal a court can review this	<i>No oversight body – appeal to courts</i>
Denmark	
FIRST Administrative Appeal THEN Appeal to Courts OR to Ombudsman	<i>Folketingets Ombudsman</i>

Appeal Options, by Country	Oversight Body
Estonia	
<p>FIRST Appeal to Supervisory body OR Administrative Court. OR Data Protection Inspectorate</p>	<i>Estonian Data Protection Inspectorate - oversees implementation of the Public Information Act</i>
Finland	
<p>FIRST Appeal to a higher authority THEN to the Administrative Court OR apply to Parliamentary Ombudsman for review of the decision</p>	<i>Parliamentary Ombudsman</i>
France	
<p>FIRST Administrative appeal (“recours gracieux”) AND/OR appeal direct to Commission on Access to Administrative Documents THEN Conseil d’État to challenge the decision of the CADA</p>	<i>Commission on Access to Administrative Documents (CADA) – decisions not binding but can appeal to Administrative Tribunal for enforcement</i>
Georgia	
<p>FIRST internal administrative appeal THEN Administrative Court THEN Supreme Court</p>	<i>No oversight body</i>

Appeal Options, by Country	Oversight Body
Germany	
<p>FIRST Administrative appeal THEN court appeal OR appeal to Information Commissioner</p>	<i>The Federal Commissioner for Data Protection and Freedom of Information Some Länder have Freedom of Information laws overseen by Commissioners: Berlin, Brandenburg, Bremen, Hamburg, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Saarland, Sachsen-Anhalt, Schleswig-Holstein</i>
Greece	
<p>FIRST Internal appeal THEN Ombudsman’s office</p>	<i>Greek Ombudsman</i>
Hungary	
<p>FIRST Applicant has option to launch judicial appeal (first and second instance) OR to appeal to the Data Protection and FOI Commissioner</p>	<i>Parliamentary Commissioner for Data Protection and Freedom of Information - decisions are not binding</i>
Iceland	
<p>FIRST Appeal to the Information Committee Government bodies are required to comply with the decisions but can appeal to the courts</p>	<i>Information Committee (In Icelandic only)</i>

Appeal Options, by Country	Oversight Body
Ireland	
FIRST Application for internal review of the decision (costs €75) THEN Appeal to the Information Commissioner (application fee of €150). THEN Appeal to High Court	<i>Office of the Information Commissioner – can order disclosure</i>
Italy	
FIRST Appeal to regional administrative court THEN Council of State	<i>Commissione Per L'accesso Ai Documenti Amministrativi</i>
Kosovo	
FIRST Internal administrative appeal THEN Administrative Court OR Ombudsman Institution	<i>Ombudsperson Institution</i>
Kyrgyz Republic	
FIRST Administrative appeal OR to the Ombudsman	<i>Ombudsman of the Kyrgyz Republic</i>
Latvia	
FIRST Appeal to manager of the institution, or to a higher institution where one exists THEN Court (takes 3-4 years and is rarely used for information requests)	<i>Latvian Ombudsman's Office – but not responsible for the access to information law!</i>

Appeal Options, by Country	Oversight Body
Liechtenstein	
FIRST Administrative appeal to the body handling the request THEN Appeal according to the administrative law	<i>No oversight body</i>
Lithuania	
FIRST Appeal to internal Appeals Dispute Commission THEN Administrative Court OR Seimas Ombudsman	<i>The Seimas Ombudsmen's Office</i>
Macedonia	
FIRST Appeal to the Information Commission THEN Administrative dispute before administrative court	<i>Commission for the Protection of the Right to Free Access to Information- can order disclosure</i>
Moldova	
FIRST Apply to top management of body and/or higher body THEN Apply to courts	<i>No oversight body</i>
Montenegro	
FIRST Appeal either to a supervisory body if one exists OR Directly to the Administrative Court, which can order disclosure	<i>No oversight body</i>

Appeal Options, by Country	Oversight Body
Netherlands	
FIRST Administrative appeal THEN Court Appeal THEN High Court Appeal	<i>(National Ombudsman: has no specific mandate so the normal appeal is via the courts)</i>
Norway	
FIRST Appeal to superior administrative body followed by appeal to courts OR to Ombudsman	<i>Sivilombudsmannen</i>
Poland	
FIRST Internal appeal THEN Administrative Court	<i>Can complain to Office of the Commissioner for Civil Rights Protection</i>
Portugal	
FIRST Committee of Access to Administrative Documents THEN Administrative Court	<i>Commission on Access to Administrative Documents</i>
Romania	
FIRST Public authority or manager THEN Administrative Court THEN Court of Appeal	<i>Courts can order disclosure. Ombudsman occasionally handles access concerns</i>
Russia	
FIRST Appeal to higher body OR to higher official according to established legal procedures THEN Appeal to Court	<i>No oversight body</i>

Appeal Options, by Country	Oversight Body
Serbia	
FIRST Administrative appeal THEN Information Commissioner THEN Administrative Court	<i>Commissioner for Information of Public Importance and Personal Data Protection - rulings are binding, final and enforceable.</i>
Slovakia	
FIRST Administrative appeal THEN Appeal to the Courts	<i>No oversight body – appeal to courts</i>
Slovenia	
FIRST Administrative appeal THEN Information Commissioner THEN Administrative Court	<i>Information Commissioner - decisions become binding upon the expiry of the term for launching an administrative dispute</i>
Sweden	
FIRST Internal appeal THEN Administrative Court of Appeal THEN Supreme Administrative Court ALSO to Parliamentary Ombudsman	<i>Parliamentary Ombudsman Riksdagens Ombudsmän - issues recommendations</i>

Appeal Options, by Country	Oversight Body
Switzerland	
<p>FIRST Appeal to Federal Data Protection and Information Commissioner for mediation</p> <p>THEN If not happy with outcome, apply for a formal decision from the public body</p> <p>THEN Appeal that decision to the federal administrative tribunal</p>	<p><i>The Federal Data Protection and Information Commissioner</i></p> <p><i>Mediates and issues recommendations which can be appealed before the courts.</i></p>
Tajikistan	
<p>FIRST Appeal to a superior officer</p> <p>OR in court</p>	
Turkey	
<p>FIRST Appeal to the Board of Review of Access to Information</p> <p>THEN Apply to Administrative Court</p>	<p><i>Board of Review of Access to Information</i></p>
Ukraine	
<p>FIRST Internal administrative appeal</p> <p>THEN Administrative Court</p>	<p><i>No oversight body</i></p>

Appeal Options, by Country	Oversight Body
UK	
<p>FIRST Administrative appeal to same body</p> <p>THEN Information Commissioner's Office</p> <p>THEN Information Tribunal, a special court which reviews ICO decisions (in Scotland judicial appeal on points of law only)</p>	<p><i>The Information Commissioner's Office (ICO)</i></p>
UK - Scotland	
<p>FIRST Administrative appeal to the same body</p> <p>THEN Review by same body</p> <p>THEN Scottish Information Commissioner</p> <p>THEN Judicial appeal, but only on a point of law</p>	<p><i>Office of the Scottish Information Commissioner</i></p>
United States	
<p>FIRST Administrative appeal, to the head of the relevant public body</p> <p>THEN to the Courts</p>	
Uzbekistan	
Can be appealed to the courts	

ANNEX E:
Access to Information Timeframes

Country	Working Days	Calendar Days	Extension
European Union	15		15
Environmental Info under Aarhus Convention		30 (one month)	
Albania		40	10
Armenia	5		25
Austria		60 (eight weeks)	
Azerbaijan	7		7
Belgium		30	
Bosnia and Herzegovina	15		15
Bulgaria		14	14
Canada		30	30 (if more, notice to be given to Info. Commissioner)
Croatia	15		30
Czech Republic	15		10
Denmark	10		allowed not specified
Estonia	5		15
Finland		14	16
France		30 (appeal after 1 month)	
Georgia	10		
Germany		30	
Greece		30	

Country	Working Days	Calendar Days	Extension
Hungary	15		
Iceland		7	
Ireland		30	
Italy		30	
Kosovo	15		15
Kyrgyzstan		15	15
Latvia	15		10
Lithuania	20		20
Liechtenstein		14	
Macedonia		30	
Moldova	15		5
Montenegro		8	14
Netherlands		28	28
Norway			
Poland		14	
Portugal	10		
Romania	10		30
Russia		30	
Serbia	15		
Slovakia	10		10
Slovenia	20		30
Sweden	immediately		

Country	Working Days	Calendar Days	Extension
Switzerland	20		
Tajikistan		30	
Turkey	15		15
Ukraine	10		30
United Kingdom	20		20
United States	20		10
Uzbekistan		30	30 (one month)

Note 1: Albania, Hungary and Romania have different time limits for decisions to grant or deny access. Time limits for decisions to deny access are shorter: 15, 8 and 5 days respectively.

Note 2: Timeframes are sometimes defined in weeks or months. For the purpose of comparability 1 month equals 30 calendar days and 1 week is 7 calendar days in the chart.

LegalLeaks

The Legal Leaks Project helps **journalists** across Europe exercise their right of access to information in their country and in other countries.

The **Legal Leaks Toolkit** is for journalists working in **any media** – newspapers, radio, and television – as well as bloggers and other information professionals who need to get access to information held by public bodies for their stories.

Based on a comparative analysis of **45 access to information laws** and the access to documents rules of the **European Union**, the Legal Leaks Toolkit includes:

- » Twenty Top Tips on the right to know for busy journalists
- » A guide on when is the right time to file an information request and how to do it
- » Tips on how to make stories out of filing requests and out of refusals
- » A step-by-step guide to all of Europe's access to information laws
- » Information on how to appeal refusals in 45 countries and at the EU level

The **Legal Leaks Toolkit** was prepared by Access Info Europe and the Network for Reporting on Eastern Europe n-ost with support from the Representative on Freedom of the Media of the Organisation for Security and Cooperation in Europe.