LegalLeaks toolkit

A guide for journalists on how to access government information

Cover photo by sïanaïs
Editors: Access Info Europe and n-ost

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 also to Marek Tuszynski of the Tactical Technology Collective and Wojtek Bogusz of Front Line Defenders. Thanks to all our partner organisations and users of the toolkit for their feedback.

www.legalleaks.info

Access Info Europe (www.access-info.org) is an international human rights organisation, founded in 2006 and based in Madrid, which promotes a strong and functioning right of access to information in Europe and globally. Access Info's advocacy, training, legal and policy analysis and standard-setting aim to make the right to information 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.org) is a Berlin-based organisation which links 250 journalists and media initiatives from more than twenty European countries. 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

CONTENTS

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 48 have legal provisions on the right of access to information held by public bodies; the law of Kosovo is also analysed. A full list of laws by date of adoption can be found in Annex A.

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 international 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. These stories can be 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.

overview: is this for me?

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 and to press your government to answer the same question.

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 IV on Data Journalism.

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 Section III on Data Security.

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 working for a media outlet, you could always write your request on your 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 plan to 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.

twenty top tips

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 contact the Legal Leaks Help Desk 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 different countries 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 possibilities. 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.legalleaks.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 comes 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 one 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, especially 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.

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.*

Pros	Cons
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.	**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.
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.	**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.
Faster: In some countries journalists get preferential treatment and to be provided with information in a shorter timeframe than other requesters.	**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.

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 and what the timeframes are. 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.

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 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 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 2011"* or *"The expenditure reports for the Ministry's purchase of IT equipment (including computers and printers) for the years 2010 and 2011."*

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 an address (postal or e-mail) are usually required. 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 to clarify anything so as 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 means either sending by post or hand-delivering a written request to the public body. In most countries you can submit requests by e-mail, as shown in Box A below. Note that in some cases e-mail requests are a matter of practice rather than law (Netherlands, Serbia). Some public bodies prefer web-based forms, but Access Info Europe argues that e-mail should always be an option as it permits the requester to keep a copy of the request.

Some access to information laws also permit oral requests, which you can make by phone or in person. 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 and timeframes are different for oral and written requests. If you don't get an immediate response, it is recommended to submit a written request so that you have record in case an appeal is necessary.

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.

BOX A: Oral Requests and E-mail Requests

Oral requests	E-mail 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.

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 or administrative law to issue a reference number to confirm that they received a letter or e-mail. Make a note of the reference number as it will be useful for chasing the request if you don't get an answer on time.

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 by cheque or postal order.

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 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 information 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 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 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.*

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.

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) 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 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 usually the first appeal letter should be sent to the information officer, to the head of the institution, or to a higher administrative body. In countries which have good access to information laws, there will be a simple and clear system for 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 contact the Legal Leaks Help Desk 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 on whether you will really appeal or not: it's not clever to say in an article or on air that you are going to appeal and then to do nothing: public authorities will get used to the empty threats and may be 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. You may also want to consult with a specialist access to information organisation and asking for their help before taking the decision.

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.*

FOIAnet

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 200 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 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 in the OSCE region to enter into force (Russia, January 2010). More details of the laws and dates can be found in Annex A and Annex B.

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

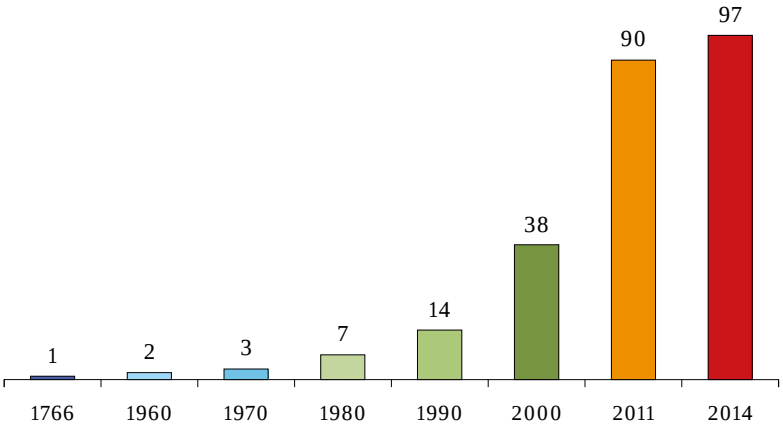
I. Proactive

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.

Figure 1: The growth of global access to information laws



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.

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.

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 international courts confirming that access to information is a human right. In the **OSCE region** 48 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, Monaco, San Marino, and Turkmenistan). Of these, 29 have constitutions which recognise a right of access to official documents or information and a total of 36 include "freedom of expression and information". Examples of the provisions on access to information in some European constitutions can be found in Box B.

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 Funtioning of the European Union** also establishes a right of access to EU documents in Article 15. This is reinforced by Article 42 of the **European Charter of Fundamental Rights** which also establishes the right of access to European Union Documents.

In 2009 the **European Court of Human Rights** 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 United Nations Human Rights Committee confirmed in July 2011 that the right to freedom of expression protected by Article 19 of the International Covenant on Civil and Political Rights includes the right of access to information. The Committee said: "*Article 19, paragraph 2 embraces a right of access to information held by public bodies. Such information includes records held by a public body, regardless of the form in which the information is stored, its source and the date of production.*"

See www.access-info.org for details.

Do you want to read all access to information laws in the world?

Check the Global Right to Information Rating to read all access to information laws and know your right.
www.rti-rating.org
There's lots of legal stuff there and you can find extracts from Constitutions from around the world.

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*" *subject only to limited exceptions.*

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.

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.

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 2004 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.

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' longest established democracy is Canada where only citizens and residents may submit requests.

In the case of the European Union, in practice anyone can make a request for information or submit a complaint to the European Ombudsman. In the EU treaties however, the right of access to documents and the right to appeal to the Ombudsman applies only to citizens, residents, and businesses registered inside the Union. While **in general** anyone **whose** right has been violated by EU institutions can appeal to the European Court of Justice, in the case of the right of access to documents, the court is only obliged to admit cases from EU citizens, residents and businesses.

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.

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*

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 Council of Europe's 2009 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 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 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 Commission/er in countries such 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. For more information see Section IV on Data Journalism.

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, Malta, Netherlands, Mongolia, Norway, Poland, Portugal, Russia, Spain, Turkey.

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 planning 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 clearly defined access to documents rules, but there is still 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 now have internal rules which are a similar to national access to information laws. These are sometimes called "disclosure policies" or "access to information policies". For example, the World Bank's Access to Information Policy 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, there are are **exceptions** to what information you can actually receive. **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 are set out in Box D below.

BOX D:
Standard Exceptions to the Right to Information

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 because of the right of partial access. 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 protected 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 is not prohibited by

law. You need to check the rules in your country. 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. Access Info Europe is campaigning for fewer restrictions on reuse of public information.

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 many countries the request for internal review is required before appealing to the Information Commissioner, Ombudsman, or Courts. Sometimes however, you can appeal directly to the Information Commissioner or Ombudsman. Box E lists these options.

» **Administrative Court Appeal:** in many countries, particularly those without an Information Commission or Ombudsman, 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 19 countries in the OSCE region 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. 16 countries in the OSCE region have a specialised oversight body. Some can issue binding decisions, others only make recommendations. The decisions of Information Commissioners can always 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 11 of these countries, the Ombudsman also has the role of receiving complaints related to the access to information requests. Often

BOX E:
Appeals mechanism in the OSCE region

Court Appeal	Information Commisson/er	Ombudsman
Austria, Azerbaijan, Bulgaria, Canada, Czech Republic, Georgia, Latvia, Liechtenstein, Moldova, Montenegro, Netherlands, Poland, Romania, Russia, Slovakia, Tajikistan, Ukraine, United States, Uzbekistan.	Belgium, Croatia, Estonia, France, Germany, Hungary, Iceland, Ireland, Italy, Macedonia, Malta, Portugal, Serbia, Slovenia, Spain, Switzerland, Turkey, United Kingdom.	Albania, Armenia, Bosnia, Denmark, Finland, Greece, Kosovo, Kyrgyz Republic, Lithuania, Mongolia, Norway, Sweden.

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.

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.

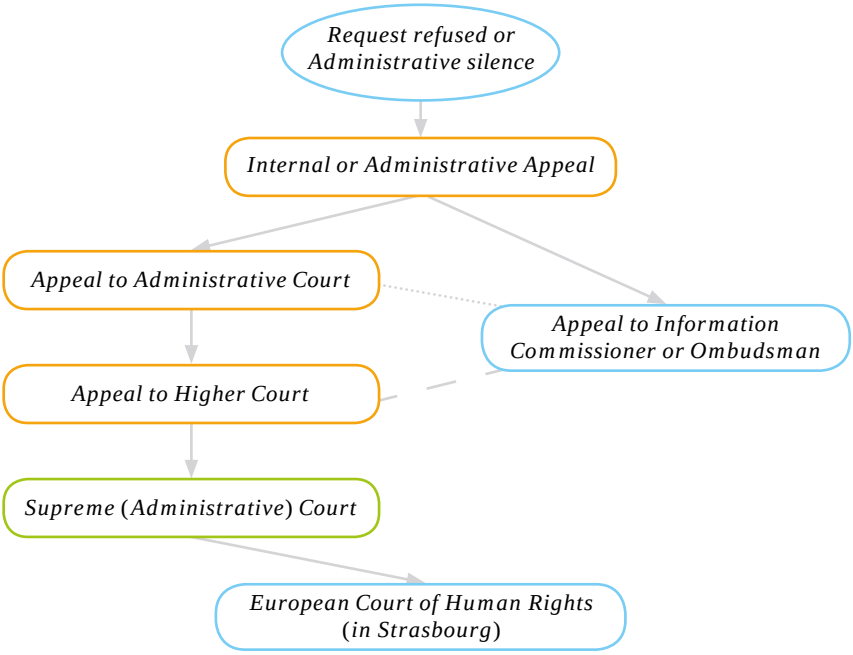
Appeals to higher courts and to the European Court of Human Rights can take a long time (even years!) but are well worth considering for two reasons:

» **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!

Figure 2: Appeals Process step-by-step

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



III. DATA SECURITY FOR JOURNALISTS

In this section we give you some tips and advice on how to protect the security of your information. For more detailed guidance go to the Security-in-a-Box toolkit by the Tactical Technology Collective (www.security.ngoinabox.org).

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

I need solutions that are not too geeky or complicated and I need to be told what to do, not to be given options because I am a busy journalist and don't have time to research this!

» **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, threats may come from 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 (For more on encrypting see Questions 3 and 5)

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 tool such as CCleaner (link provided in the Security-in-a-Box toolkit).

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. The steps to follow are in the Security-in-a-Box toolkit.

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?** Skype voice and text communications are encrypted. The history of calls that you made and of the text messages you exchanged is stored on your computer and the on the computer of your contact. As Skype is not open source software it is not clear if communications are retained anywhere else.
» **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. Make sure that your computer is virus and spyware free. Always independently verify the identity of a person that you are communicating with. Be careful of what you say, wiretapping maybe done on different levels (also at the physical level of the headphones/microphone or a bug in your room or that of the other person). Consider developing a code system for what you say to each other.

Note: Skype calls to fixed or mobile phones fall into the domain of phone networks, which are typically NOT

secure. You should also be aware that in some countries Skype is less secure. This is the case in China for example for users of TOM-Skype which is Skype's distribution inside China.

4. Using mobile phones

How risky is it to use a mobile phone?

» **You should assume that all standard phone communication is NOT secure.** Both voice and text communication can be accessed by phone companies and third parties at any given time. Your phone is an excellent tracking device, which can easily be turned into a spying device. See Security-in-a-Box Chapter 9 for details on how to use mobile phones as securely as possible.

» **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. Don't save sensitive information on your mobile phone, or if you have to, "obfuscate" it so only you can understand it. You should regularly delete unwanted and/or sensitive information on your phone.

» **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 on eHow.com: How to Stop Phone Tapping.

» **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 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. Use circumvention tools to create and access your e-mail account. See Security-in-a-Box Chapter 8 on How to remain anonymous and bypass censorship on the internet.

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 (installation and use instructions in Security-in-a-Box).

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. See Security-in-a-Box Chapter 3 on How to create and maintain secure passwords.

» **Use a password manager** that allows you to store passwords securely and also allows you to generate more complex passwords automatically. When using a password manager you only need to remember one (1) secure password: a master password. It unlocks your password manager so you will have access to your other passwords. Please refer to Security-in-a-Box Chapter 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 e-mail 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 Security-in-a-Box Chapter 7.

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.

» **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. 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 sever, 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 when accessed both inside and 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. Use dedicated e-mail accounts for communicating with a single source.

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

TIP! ***Avoid sharing e-mail accounts with other people*** *– it makes managing security impossible.*

TIP! ***Keep an eye on address bar of your browser*** *to check that you are not being redirected to some other website.*

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.

8. 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. If you independently encrypt your content you may consider using online offsite backups. However note that this will give third parties access to your encrypted data.

» **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 (See previous Questions).

» **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 a trusted 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.

9. 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 can choose to make a private or a public Google map. The extent to which this assertion can be verified, 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 End-User Licence Agreements (EULAs) of these tools. It is impera-

tive 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). Use 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 (see transmission security in Question 7 above).

10. 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 must consider information put on and communicated over Facebook or sent by Twitter as public.** You should keep your privacy settings turned up high on those sites. But be aware that the information has been shared. 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.

» **Can I have a "private" blog?** *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?*

It is possible to install your own server computer and keep information on it as private as you can. But it requires skills, resources and management. You can use online services providing private configuration settings (Google, WordPress). Note that once you use someone else's service you give access to your information to owners of the services you use.

11. 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!

12. 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 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 and/or always use encrypted connections (https) and only use your own security prepared laptop.

» **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 paper 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/

IV. DATA JOURNALISM & THE RIGHT TO KNOW

1. What is data journalism?

Modern information and communication technologies are helping journalists gain access to ever-larger quantities of information. The use of computers makes it easier to sort through that information in search of new leads or the evidence that justifies a story.

Data journalism is the use by journalists of large quantities of information, be it numbers or other types of data, to identify or to back up a story.

Data Journalism includes the analysis of data sets using computer software programmes, ranging from simple spreadsheets such as Excel to the advanced data processing and data visualisation tools.

These computer tools make it easier to do new and exciting things with data sets: to combine, compare, sort, and analyse large volumes of data very quickly, to produce summaries and visualisations which help you to gain new perspectives and to see patterns in the data which would otherwise be invisible. And they allow you to communicate these patterns to the public in ways that make them easily understandable.

In many ways, data journalism is simply traditional journalism using new tools: the progression from "pen and paper assisted reporting", to "telephone assisted reporting" to "computer assisted reporting" does not change the fundamentals of the profession of journalism but does require that a good journalist masters the available tools.

There is also no essential difference between data journalism and computer assisted reporting: one term focuses on the tool – the computer – the other term on the material, the data.

Data journalism requires three skills:

- The ability to get hold of the data;
- The ability to organise the data;
- The ability to analyse the data.

This section looks at the kind of data that is available to journalists, the possible sources of that data, and where to go to get further advice and training on the skills needed to organise and analyse the data.

2. Where do I get my data from?

Depending on the kind of story that you as a journalist are working on, there will be a variety of sources of information and data.

» **Public datasets:** public bodies are now publishing on the internet full datasets, including statistical information, detailed records of public spending, and other information about the services they provide and the information collected in the course of government functions. Increasingly these are released on public data portals (see the online version of the Legal Leaks Toolkit at Section IV for details and links).

» **Public information not in database format:** there is a lot of information that is published on government websites or which can be obtained through information requests which does not come in database format but which you can convert into that format. For example, suppose that you have asked all the ministries in your country for details of the interest groups (private business associations, lobby groups, and NGOs) that they have met with over the past year. You have all this information in documents sent by each public body. To be able to analyse it you might put it into a spreadsheet, with columns for the name of the public body, the name of the organisation, the name of the representatives in the meeting, the dates of the meetings, and other information you have. Once this is in the spreadsheet, it is a dataset that you can start working with.

» **Data from private sources:** There are multiple private sources of information which you can get through your contacts or because the information is published. Non-governmental organisations often do a lot of research and the datasets that they collate can be a valuable source for making more of a story than a simple press release. Businesses these days run on large databases: a business may be willing to share its data with you if they understand the story you are working on (and possibly have an interest in helping make a certain situation more transparent). Similarly academics often compile huge volumes of data which are not always used in academic papers but which can be of great value for cross referencing elements of your story and helping you analyse public datasets with complementary or even contradictory information.

» **Data from your own observations:** You might have access to a dataset from a public authority, for example you have collected your own data on anything from the location of rubbish bins in your town to information from the media about the number of foreign trips made by ministers. You can organise this data in a spreadsheet and combine it with other information obtained from public or private sources.

TIP! ***Explore the data governments are releasing and find out what is available:*** *If your government has recently set up an open data portal, it's well worth taking the time to surf around it and find out what kind of information is there. Think creatively and you might find an unexpected story in newly released data sets. Or you might find that very little of the information is new or up to date, which could be another kind of story.*

3. Do I have a right to public data?

Yes! You should have the right of access to the detailed information that is being used by public bodies for public policy and decision making. However, many laws were written before the recent **"open data revolution"** and do not clearly state that there is a right of access to full datasets.

As was noted in Section II Point 5 of the Legal Leaks toolkit, some laws refer to the right of access to information and we noted that some laws refer to a right of access to documents; there is then a question of whether the definition of information or documents includes databases and it's important to check the definition in the law of the country where you want to make a request. The information in Annex F on whether you have a right to electronic information and to databases should help you with this.

With the rise of the open government data movement there is now a trend to talk about the "Right to Data" which is sometimes presented as being different from or additional to the right of access to information.

The Legal Leaks team of Access Info Europe and n-ost does not believe that a "right to data" is strictly necessary because all information held by public bodies should already be accessible under the right of access to information. There are however some positive elements in this reframing of the right because it makes clear that:

» Detailed information should be available in a "disaggregated" or "granular" format – this is sometimes also referred to as "raw data" before it has been "cooked" by public officials and statisticians;

» Entire datasets or databases should be made available, in an open source and machine readable format in order to permit re-use of the information.

TIP! ***Check for precedents:*** *Find out that some databases have already been released in your country under the access to information law, use this to argue in favour of release of other databases. Your national access to information NGO or the information commissioner or ombudsman should be able to help you with this.*

TIP! ***If you already have a story, know in advance exactly what data set you want:*** *Just as with a good information request, it helps to be clear and accurate when requesting access to a database. Most access to information laws do not require requesters to indicate the exact document they are looking for, but it certainly helps if you are requesting access to a database to know that it exists. One way to check this is to file an initial request asking which databases a public authority holds – or just phone them up and ask them before sending off the request.*

Another way is to ask an experts such as an academic or NGO what kind of databases might be available to help you with your story.

4. What about charges for access to databases?

In spite of the open government data movement that is currently sweeping around the world, many public authorities still see large datasets as valuable assets to be monetised for maximum return.

In Europe there used to be a tradition of selling databases to one single company which would then republish the information (for example, laws and jurisprudence) or for the public body or semi-privatised public body to package and sell the information (such as statistical information sold in books or geospatial data used to make maps for sale by the state mapping office to the public).

To try to break these monopolies, the EU adopted the Directive on the Re-use of Public Sector Information. This has helped in some ways but has created problems in other ways: in some cases it has encouraged public bodies to think of their databases as a commodity to be marketed sometimes for tens of thousands of Euros, which could mean that the information is out of the price range of the average journalist or small media outlet.

This problem is complicated further in countries where public information is considered to be the intellectual property of governments and is protected by copyright or intellectual property rights.

Access Info Europe and n-ost argue that there should never be charges for public databases, particularly when they are being used for public interest reasons such as that a journalist is writing a story with the information.

TIP! ***Insist on your right to public information free of charge:*** *Use your access to information right to obtain the database and challenge the public authority if they try to impose a large fee or other licence or copyright for accessing the information. If you are still having problems, contact the Legal Leaks Help Desk and we will give you advice on filing a legal appeal for access to the information.*

5. What kind of formats do I need?

To run analyses on the data, you need it to be in a form and format which permits you to work with it, to combine it with other data sets, and to use data visualisation tools.

It is not enough that data is in a digital format such as a locked .pdf file. The data also needs to be in a format that ensures that it is reusable.

Given that nowadays most information is created and stored digitally, it is advi-

sable when requesting the information to request it in the format in which it was originally stored. Although many public bodies prefer to send out information in locked formats such as a .pdf because they believe that makes it seem more "finished" and "formal", this makes your work more difficult, slowing it down, and increasing the risk of making mistakes or corrupting the data when converting the data to a spreadsheet or other format. These are good reasons for insisting on your right to the data in its original format.

Another problem you might have is that the public authority says that they hold the data in a database which was constructed by a private company, is protected by copyright, and therefore cannot be shared for this reason, or you cannot have it unless you also buy some very expensive software licence. Sometimes this is the case and you have various options:

» Try insisting that the public authority converts the data into a format which can be read by open source software;

» Make a story out of the fact that information which should belong to the public is locked up in proprietary formats rather than being freely accessible;

» Contact an NGO or local open data activists and ask them to help you campaign for access to the database;

» Take a case to the information commissioner, ombudsman or courts – the Legal Leaks Help Desk can give you advice on this.

6. What skills do I need?

Journalists have always needed analytical skills, and the ability to organise, process and evaluate information. This doesn't change with data journalism, although the ability to use some basic computer programmes greatly helps speed up the work that previously might have been done by sifting through large piles of paper and making notes in order to get meaning out of it and to identify trends and patterns.

There is a myth that data journalism requires good mathematical skills, but those who were always bad at maths need not worry: the use of spreadsheets and other computer tools means that you no longer need to be able to add up or do long division in your head. What you do need, however, are the analytical skills to see that in some cases two plus two very definitely adds up to more than four, and when that happens, you have a story! There are, however, some things you can do to improve your skill set and to make sure you can use the key data journalism tools:

» A good understanding of spreadsheets such as Excel, Open Calc, and similar, is pretty essential for manipulating data, and Google Refine is recommended for cleaning up mess databases.

» Taking time to familiarise yourself with the relevant terminology in the fields of statistics and computing is also worthwhile so that you don't feel overwhelmed or confused by the jargon.

» Similarly finding a data visualisation tool that you like and enjoy working with is recommended. The International Journalist's Network recommends three starter tools: ManyEyes, Vuvox, and Dipity.

» The ability to "scrape" data off public website (see also note on scraping below). Working with a person with technical skills or learning some yourself is essential here. There are good websites such as ScraperWiki.com where you can make contact with developers and data visualisers.

The online version of the Legal Leaks Toolkit has more information and links to useful web pages and key data journalism resources.

7. Is it legal to scrape the websites of public bodies?

As public bodies put more information on their websites, it's easier for journalists to download either whole data sets or to "scrape" the data off a website bit by bit.

Scraping is the gathering of data from a website using a computer or automated program when the data is not specifically designed for downloading. For example, you may be able to search your national companies register page by page, record by record, but not download the entire database. Or you may go to a database of laws or court records which are in PDF format, download them one by one, convert them to another format (Open Office for example) and then put them all together in one document or a database.

Increasingly journalists are getting the information they need in this way.

The question is, is it legal?

Essentially this depends on two things: the legal framework in your country and the specific terms of use of the website from which you are collecting the data.

Sometimes the national access to information law will make clear that all public information is in principle accessible to the public. This means that if it has been published, it should be free to use. Even in countries without an access to information law this should be the case.

There are however exceptions. In some countries there is copyright on public documents, so that even if they are public, you cannot reuse them without permission. Check the terms and conditions of a website for the intellectual property limitations: often the only requirement is that you cite the source of the information.

Then there is the issue of government bodies selling entire datasets. This is the case, for example, with many company registers: you can check some records for free but to have access to the entire database you need to pay.

Some websites make clear a distinction between commercial use of the information and use for other purposes: non-commercial use only being free. This is a bit of a grey area where journalists are concerned, because most media outlets are in fact commercial.

Access Info Europe and n-ost believe that this runs counter to the principle of freedom of expression, especially when you are a journalist using the information to report on matters of public debate.

But there is a real possibility that if you scrape data and then use it you might be charged for it later or have legal action taken against you or your media outlet. For these reasons it's best to check very carefully and possibly talk to an access to information or other lawyer before using the information.

If you find you are having problems with your right to reuse information, then please let **Legal Leaks Help Desk** know (helpdesk@legalleaks.info). We will help you with legal advice and will try to find lawyers in your country should that be necessary.

ANNEX A:
Adoption of Access to Information Laws 1766-2013

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, New Zealand, Canada, Colombia, Greece, Austria, Italy	7	14
1991-2000	Hungary, Ukraine, Belgium, Belize, Iceland, South Korea, Ireland, Thailand, Israel, Latvia, Albania, Portugal, Czech Republic, Georgia, Japan, Liechtenstein, Trinidad & Tobago, Bulgaria, Estonia, Lithuania, Moldova, Slovakia, South Africa, United Kingdom	24	38
2001-2013	Bosnia & Herzegovina, Poland, Romania, Angola, Jamaica, Mexico, Pakistan, Panama, Uzbekistan, Zimbabwe, Armenia, Croatia, Kosovo, Peru, Slovenia, St Vincent and the Grenadines, Switzerland, Antigua and Barbuda, Argentina, Dominican Republic, Ecuador, Serbia, Turkey, Azerbaijan, Germany, India, Montenegro, Taiwan, Uganda, Honduras, Macedonia, China, Cook Islands, Jordan, Kyrgyz Republic, Nepal, Nicaragua, Bangladesh, Chile, Ethiopia, Guatemala, Malta, Indonesia, Tajikistan, Uruguay, Russia, Guinea-Conakry, Liberia, El Salvador, Mongolia, Niger, Nigeria, Tunisia, Brazil, Yemen, Sierra Leona, Rwanda, Guayana, Spain	59	97

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 in Official Documents	1999
Armenia	Law of the Republic of Armenia 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	Law on the Right of Access to Administrative Documents	1994
Bosnia and Herzegovina	Freedom of Access to Information Act for the Federation of Bosnia and Herzegovina	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 Administrative Documents Act	1985
Estonia	Public Information Act	2000
Finland	Act on the Openness of Government Activities	1999

Access to Information Laws in the 56 OSCE Participating States

Country	Name of the Act	Year
France	Law 78-753 of 17 July 1978 on Freedom of Access to Administrative Documents and the Reuse of Public Information	1978
Georgia	Law of Georgia "On Freedom of Information" – The General Administrative Code of Georgia	1999
Germany	Federal Act Governing Access to Information held by the Federal Government – (Freedom of Information Act)	2005
Greece	Law No 2690 – Administrative Procedure Code	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	1997
Italy	New rules on administrative procedure and right to access to administrative documents, Law 241/90	1990
Kosovo	Law on Access to Public 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

Access to Information Laws in the 56 OSCE Participating States

Country	Name of the Act	Year
Lithuania	Law on Provision of Information to the Public (No. I-1418)	1996
Macedonia	Freedom of Information Act	2008
Moldova	Law on Access to Information	2000
Mongolia	The Law of Mongolia on Information Transparency and Right to Information	2011
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
Poland	Act on Access to Public Information	2001
Portugal	Law on Access to and Re-Use of Administrative Documents (Law no. 46/2007)	2007
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

Access to Information Laws in the 56 OSCE Participating States

Country	Name of the Act	Year
Slovenia	Act on the Access to Information of Public Character	2003
Spain	Law 19/2013, of the 9th of december, on Transparency, Access to Public Information and Good Governance	2013
Sweden	Freedom of the Press Act	1766
Switzerland	Federal Act on the Principle of Freedom of Information in Public Administration	2004
Tajikistan	Law Republic of Tajikistan on the Right to Access to Information	2002
Turkey	Law on the Right to Information (No. 4982)	2003
Ukraine	Law on Public Access to Information	2011
United Kingdom	Freedom of Information Act	2000
United States	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	Yes	Yes
Armenia	Yes	Yes	Partially	Yes	Yes
Austria	Yes	Yes	Yes	Yes	No
Azerbaijan	Yes	Only Leg.	Yes	No	Yes
Belgium	Yes	Yes	No	No	Yes
Bosnia & Herzegovina	Yes	Yes	Yes	Yes	Yes
Bulgaria	Yes	Yes	Yes	Yes	Yes
Canada	Yes	No	No	No	No
Croatia	Yes	Yes	Yes	Yes	Yes
Czech Republic	Yes	Yes	Yes	Yes	Yes
Denmark	Yes	Yes	Yes	No	Yes
Estonia	Yes	No	No	No	Yes
Finland	Yes	Yes	Yes	Yes	Yes
France	Yes	No	No	Yes	Yes
Georgia	Yes	Yes	Partially	Yes	Yes
Germany	Yes	Yes	No	No	Yes
Greece	Partially	Partially	No	No	No

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
Hungary	Yes	Yes	Yes	Yes	Yes
Iceland	Yes	No	No	No	Yes
Ireland	Yes	Yes	Partially	No	Yes
Italy	Yes	Yes	No	No	Yes
Kosovo	Yes	Yes	Partially	Partially	Yes
Kyrgyz Republic	Yes	Yes	Yes	Yes	Yes
Latvia	Yes	Yes	No	No	Yes
Liechtenstein	Partially	Yes	Partially	Partially	Yes
Lithuania	Yes	Yes	Yes	Yes	Yes
Macedonia	Yes	Yes	Yes	Yes	Yes
Malta	Partially	Yes	Partially	Partially	Yes
Moldova	Yes	Yes	Yes	Yes	Yes
Mongolia	Partially	Yes	Partially	Yes	Yes
Montenegro	Yes	Yes	Yes	Yes	Yes
Netherlands	Yes	No	No	No	No
Norway	Yes	No	No	No	Yes
Poland	Yes	Yes	Yes	Yes	Yes

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
Portugal	Yes	Yes	No	No	Yes
Romania	Yes	Yes	Yes	Yes	Yes
Russia	Yes	Yes	Partially	Partially	No
Serbia	Yes	Yes	Yes	Yes	Yes
Slovakia	Yes	Yes	Yes	Yes	Yes
Slovenia	Yes	Yes	Yes	Yes	Yes
Spain	Partially	Only Leg.	No	No	No
Sweden	Yes	Yes	Yes	Yes	Yes
Switzerland	Yes	Only Leg.	Yes	No	Yes
Tajikistan	Yes	Yes	Yes	Yes	No
Turkey	Yes	Yes	Yes	Yes	No
Ukraine	Yes	Yes	Yes	Yes	Yes
United Kingdom	Yes	Yes	Yes	No	Yes
United States	Yes	No	No	No	No
Uzbekistan	Yes	Yes	Yes	Yes	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	European Ombudsman
Albania	
FIRST Administrative appeal **THEN** Judicial appeal **OR** complaint to Ombudsman	People's Advocate (Ombudsperson) – decisions are not binding
Armenia	
FIRST Administrative appeal followed by appeal to the Courts (recommended) **OR** Ombudsperson	Human Rights Defender of the Republic of Armenia (Ombudsperson) – decisions are not binding
Austria	
FIRST Administrative appeal **THEN** Appeal to the Courts	Austrian Ombudsman Board
Azerbaijan	
FIRST Appeal to authorized agency on information matters **OR** Appeal to Courts	Authorized Agency on Information Matters

Appeals Options and Oversight Bodies

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 (not binding) **THEN** application to Administrative Court for annulment of refusal to grant information	Federal Commission on Access to Administrative Documents Commission
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	Appeal Instance on access to administrative documents and the re-use of public sector information
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	Commission on Access to Administrative Documents for the French Community of Belgium
Bosnia Herzegovina	
FIRST Appeal to head of the public authority that issued the decision **THEN** apply for judicial review **OR** complaint to Ombudsman	Ombudsman for Human Rights
Bulgaria	
ONLY (depending the body) Regional courts or Supreme Administrative Court	No oversight body – appeal to courts

Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
Canada	
FIRST Complaint to Information Commissioner **THEN** Appeal to the courts	Office of the Information Commissioner of Canada
Croatia	
FIRST Administrative appeal to head of the administrative body **THEN** Administrative court **OR** Croatian Personal Data Protection Agency	Croatian Personal Data Protection Agency
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	No oversight body – appeal to courts
Denmark	
FIRST Administrative Appeal **THEN** Appeal to Courts **OR** to Ombudsman	The Parliamentary Ombudsman
Estonia	
FIRST Appeal to Supervisory body **OR** Administrative Court **OR** Data Protection Inspectorate	Estonian Data Protection Inspectorate
Finland	
FIRST Appeal to a higher authority **THEN** to the Administrative Court **OR** apply to Parliamentary Ombudsman for review of the decision	Parliamentary Ombudsman

Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
France	
FIRST Administrative appeal ("recours gracieux") (optional) **AND/OR** appeal direct to Commission on Access to Administrative Documents **THEN** Conseil d'État to challenge the decision of the CADA	Commission on Access to Administrative Documents (CADA) – decisions not binding but can appeal to Administrative Tribunal for enforcement
Georgia	
FIRST internal administrative appeal **THEN** Administrative Court **THEN** Supreme Court	No oversight body
Germany	
FIRST Administrative appeal **THEN** Court appeal **AND/OR** appeal to Information Commissioner	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
Greece	
FIRST Internal appeal **THEN** Ombudsman's office	Ombudsman

Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
Hungary	
FIRST Applicant has option to launch judicial appeal (first and second instance) **OR** to appeal to the National Data Protection and Freedom of Information Authority	National Data Protection and Freedom of Information Authority - decisions not binding
Iceland	
FIRST Appeal to the Information Committee Government bodies are required to comply with the decisions but can appeal to the courts **THEN** Appeal to the courts	Information Committee
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	Office of the Information Commissioner – can order disclosure
Italy	
FIRST Appeal to regional administrative court **OR** Appeal to Access to Information Commissioner **THEN** Appeal to court	Commission for access to administrative documents
Kosovo	
FIRST Internal administrative appeal **THEN** Administrative Court **OR** Ombudsperson Institution	Ombudsperson Institution
Kyrgyz Republic	
FIRST Administrative appeal **OR** to the Ombudsman	Ombudsman of the Kyrgyz Republic

Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
Latvia	
FIRST Appeal to manager of the institution, or to a higher institution where one exists **THEN** Court	No oversight body
Liechtenstein	
FIRST Administrative appeal to the body handling the request **THEN** Court according to the administrative law	No oversight body
Lithuania	
FIRST Internal Appeal (optional) **OR** Administrative Dispute Commission (optional) **THEN** Administrative Court **OR** Seimas Ombudsman	The Seimas Ombudsmen's Office
Macedonia	
FIRST Appeal to the Information Commission **THEN** Administrative dispute before administrative court	Commission for the Protection of the Right to Free Access to Information – can order disclosure
Malta	
FIRST Appeal to Oversight body	Commissioner of Information
Moldova	
FIRST Apply to top management of body and/or higher body **THEN** Apply to courts	No oversight body

Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
Mongolia	
FIRST Appeal to the Institution **SECOND** The National Human Rights Commission of Mongolia **THIRD** to the courts	National Human Rights Commission of Mongolia
Montenegro	
FIRST Appeal either to a supervisory body if one exists **OR** Directly to the Administrative Court, which can order disclosure	No oversight body
Netherlands	
FIRST Administrative appeal **THEN** Court Appeal **THEN** High Court Appeal	National Ombudsman: has no specific mandate so the normal appeal is via the courts
Norway	
FIRST Appeal to superior administrative body followed by appeal to courts **OR** to Ombudsman	The Parliamentary Ombudsman – the Sivilombudsmannen
Poland	
FIRST Internal appeal **THEN** Administrative Court	Can complain to Office of the Commissioner for Civil Rights Protection
Portugal	
FIRST Committee of Access to Administrative Documents **THEN** Administrative Court	Commission on Access to Administrative Documents

Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
Romania	
FIRST Public authority or manager **THEN** Administrative Court **THEN** Court of Appeal	Courts can order disclosure. Ombudsman occasionally handles access concerns
Russia	
FIRST Appeal to higher body **OR** to higher official according to established legal procedures **THEN** Appeal to Court **OR** Prosecutor's Office	No oversight body
Serbia	
FIRST Administrative appeal **THEN** Information Commissioner **THEN** Administrative Court	Commissioner for Information of Public Importance and Personal Data Protection – rulings are binding, final and enforceable
Slovakia	
FIRST Administrative appeal **THEN** Appeal to the Courts	No oversight body – appeal to courts
Slovenia	
FIRST Administrative appeal **THEN** Information Commissioner **THEN** Administrative Court	Information Commissioner – decisions become binding upon the expiry of the term for launching an administrative dispute

Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
Spain	
FIRST Appeal to the Council for Transparency and Good Governance **THEN** to the courts	Council for Transparency and Good Governance
Sweden	
FIRST Internal appeal **THEN** Administrative Court of Appeal **THEN** Supreme Administrative Court **ALSO** to Parliamentary Ombudsman	Parliamentary Ombudsman Riksdagens Ombudsmän – issues recommendations
Switzerland	
FIRST Appeal to Federal Data Protection and Information Commissioner for mediation **THEN** If not happy with outcome, apply for a formal decision from the public body **THEN** Appeal that decision to the federal administrative tribunal	The Federal Data Protection and Information Commissioner mediates and issues recommendations which can be appealed before the courts
Tajikistan	
FIRST Appeal to a superior officer **OR** in court	
Turkey	
FIRST Appeal to the Board of Review of Access to Information **THEN** Apply to Administrative Court	Board of Review of Access to Information
Ukraine	
FIRST Internal administrative appeal **THEN** Administrative Court	No oversight body

Appeals Options and Oversight Bodies

Appeal Options, by Country	Oversight Body
UK	
FIRST Administrative appeal to same body **THEN** Information Commissioner's Office **THEN** Information Tribunal, a special court which reviews ICO decisions (in Scotland judicial appeal on points of law only)	The Information Commissioner's Office (ICO)
UK - Scotland **FIRST** Administrative appeal to the same body **THEN** Review by same body **THEN** Scottish Information Commissioner **THEN** Judicial appeal, but only on a point of law	Office of the Scottish Information Commissioner
United States	
FIRST Administrative appeal, to the head of the relevant public body **THEN** to the Courts	
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[1]		40	10
Armenia	5		25
Austria		60 (eight weeks)	
Azerbaijan	7		7
Belgium		30	
Bosnia & Herzegovina	15		15
Bulgaria		14	10
Canada[2]		30	30
Croatia	15		30
Czech Republic	15		10
Denmark	10		Allowed but time limit not specified
Estonia	5		15
Finland	10		20

Access to Information Timeframes

Country	Working Days	Calendar Days	Extension
France		30 (appeal after 1 month)	
Georgia	10		
Germany		30	
Greece		30	
Hungary[1]	15		
Iceland		7	
Ireland		30	
Italy		30	
Kosovo	15		15
Kyrgyzstan		15	15
Latvia	15		10
Lithuania	20		20
Liechtenstein		14	
Macedonia		30	
Malta	20		20
Moldova	15		5

Access to Information Timeframes

Country	Working Days	Calendar Days	Extension
Montenegro		8	14
Mongolia	7		7
Netherlands		28	28
Norway			
Poland		14	
Portugal	10		60 (two months)
Romania[2]	10		30
Russia		30	15
Serbia	15		
Slovakia	10		10
Slovenia	20		30
Spain		30	30
Sweden	Immediately		
Switzerland	20		20
Tajikistan		30	
Turkey	15		15

Access to Information Timeframes

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

Note 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.

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 In Canada extensions of more than 30 calendar days are permitted but in these cases notice must be given to the Information Commissioner.

ANNEX F:
Electronic Formats and the Right of Access to Databases

Country	Access in electronic format	Access to databases
Albania	Yes, format option	Not mentioned
Armenia	Yes	Not mentioned
Austria	Not mentioned	Not mentioned
Belgium	Not mentioned	Not mentioned
Bosnia	Yes, format option	Not mentioned
Bulgaria	Yes	Not mentioned
Canada	Not mentioned	Not mentioned
Croatia	Not mentioned	Not mentioned
Denmark	Not mentioned	Specifically excluded
Estonia	Yes	Not mentioned
EU	Yes	Not mentioned
Finland	Yes	Yes
France	Yes	Not mentioned
Georgia	Yes, format option	Not mentioned
Germany	Yes	Not mentioned
Greece	Not mentioned	Not mentioned
Hungary	Yes	Only with relation to data protection
Ireland	Yes	Yes

Electronic Formats and the Right of Access to Databases

Country	Access in electronic format	Access to databases
Italy	Not mentioned	Not mentioned
Kosovo	Yes	Not mentioned
Latvia	Yes, format option	Not mentioned
Macedonia	Yes	Not mentioned
Malta	Yes	Not mentioned
Moldova	Yes	Not mentioned
Mongolia	Yes	Not mentioned
Montenegro	Yes	Not mentioned
Netherland	Yes	Specifically excluded
Norway	Yes	Not clear
Poland	Yes, format option	Not mentioned
Portugal	Yes	Not mentioned
Romania	Not mentioned	Not mentioned
Serbia	Yes	Not mentioned
Slovakia	Yes	Not mentioned
Slovenia	Yes	Not mentioned
Spain	Yes	Not mentioned
Switzerland	Yes	Not mentioned

Electronic Formats and the Right of Access to Databases

Country	Access in electronic format	Access to databases
Sweden	Yes	Only access in printed format
United Kingdom	Yes	Not mentioned
United States	Yes	Not mentioned

LegalLeaks

www.legalleaks.info

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 **46 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.
- Tips on how to keep your data safe.
- Data journalism and access to information.
- A step-by-step guide to all of Europe's access to information laws.
- Information on how to appeal refusals in 46 countries and at the EU level.

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

access !Nfo
www.access-info.org

n-ost
Network for Reporting on Eastern Europe

OSCE