

# Conducting Expert Calls Under

---

# GDPR



## INTRODUCTION

Not a lot has been written on the topic of expert networks and the General Data Protection Regulation, GDPR. In an industry that has been plagued by insider trading scandals, and where robust compliance processes are a primary selling point, this is a bit surprising.

The Internet is flooded with general articles and advice on how to achieve GDPR compliance. However, the protection of personal data when conducting expert calls is an often overseen topic.

But who bears the responsibility for the processing of the expert's personal data when planning and conducting expert calls?

This guide is meant as an introduction to the GDPR for individuals and organizations who are involved with expert calls, as clients or suppliers.

# INDEX

<b>INTRODUCTION</b>	<b>1</b>
<b>SOURCING EXPERTS</b>	<b>3</b>
The role of the expert network	
<b>CONDUCTING EXPERT CALLS</b>	<b>6</b>
The role of the client	
<b>BEING A DATA CONTROLLER</b>	<b>10</b>
Obligations and responsibilities	
<b>BEING A DATA PROCESSOR</b>	<b>16</b>
Obligations and responsibilities	
<b>GDPR IS A GLOBAL CONCERN</b>	<b>20</b>
<b>PUTTING PRIVACY FIRST</b>	<b>23</b>
How Inex One supports your GDPR compliance efforts	
<b>ABOUT INEX ONE</b>	<b>25</b>

*Legal disclaimer: All information in this guide is general information only. It is not intended to constitute legal advice, nor is it intended to address your specific requirements. Organizations should take independent legal advice regarding their own provisions for data protection.*



## WHAT YOU NEED TO KNOW

01. The GDPR came into effect on May 25, 2018.

02. It's the most comprehensive piece of privacy legislation developed by any jurisdiction to date.

03. Any business that holds, controls or processes data of EU residents is affected - even if they're established outside of the EU.

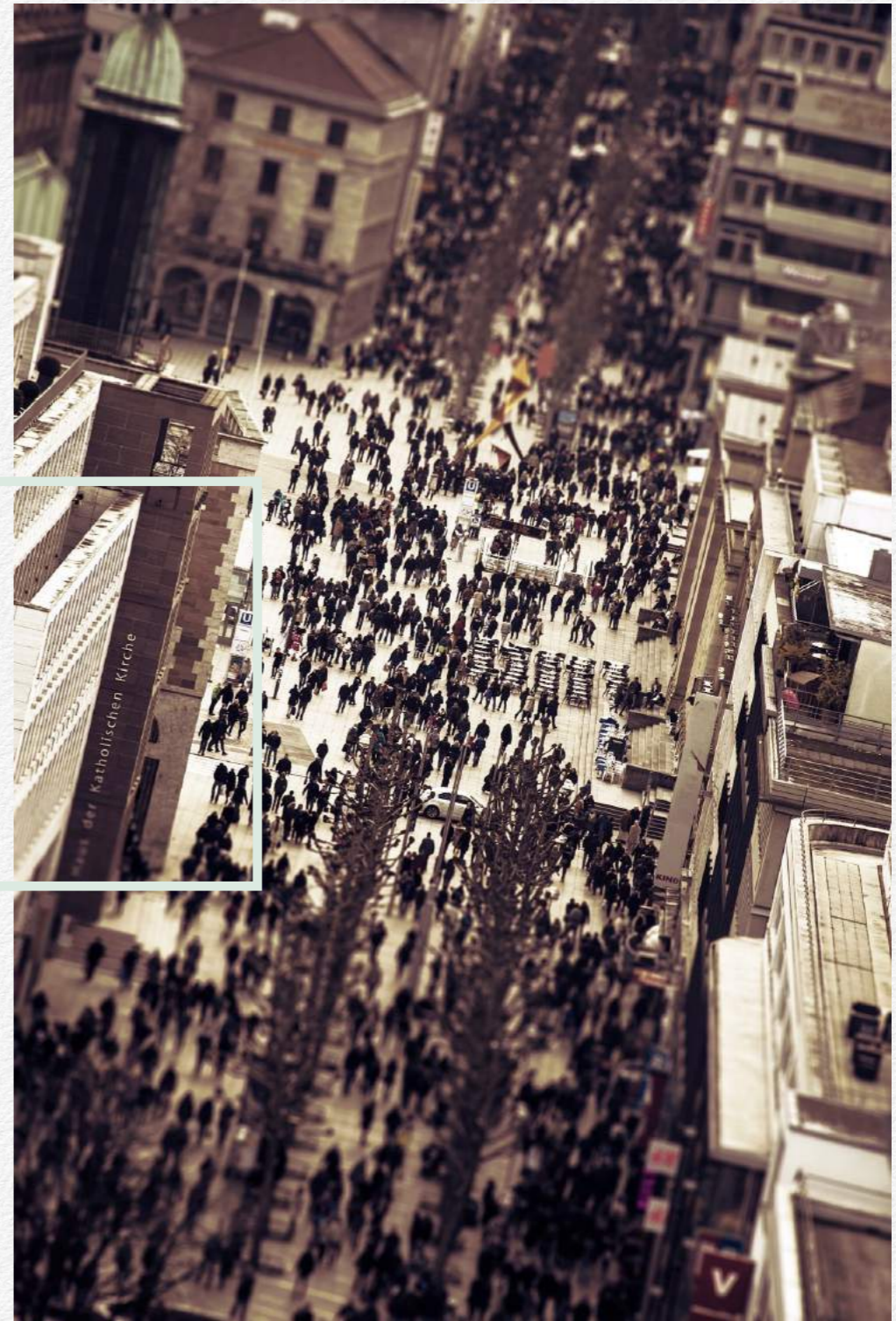
04. Non-compliance can be fined with up to €20 million or 4% of global turnover (whichever is highest). And maybe more importantly, non-compliance can severely damage a company's brand and reputation.

05. 'Personal data' is a broad concept under GDPR, and also indirectly identifiable information like career history is included in the definition.

# 1

## SOURCING EXPERTS

*- The role of the expert network*



---

## DEFINITIONS

**01. PERSONAL DATA:** any information relating to an identified or identifiable natural person.

**02. DATA SUBJECT:** a natural person who can be identified, directly or indirectly.

**03. DATA CONTROLLER:** the natural or legal person which, alone or jointly with others, determines the purposes and means of the processing of personal data.

**04. DATA PROCESSOR:** a natural or legal person which processes personal data on behalf of the controller.

**05. SUB-PROCESSOR:** a third party data processor engaged by a processor.

**06. RECIPIENT:** a natural or legal person, to which the personal data are disclosed, whether a third party or not (depending on the circumstances, the recipient may also be a controller or processor).

**As established in the introduction of this guide**, not a lot has been written on the topic of expert networks and GDPR.

However, there's another closely related industry that can be used as an analogy; headhunting and recruitment. After all, expert networks are acting as headhunting firms, chasing the best candidates for very short job assignments.

**So which role does the expert network take** when processing the personal data of experts they recruit to provide consultations to clients? Well, when it comes to recruitment, most sources agree; *the job candidate is a data subject*, and *the recruitment firm is a data controller*.

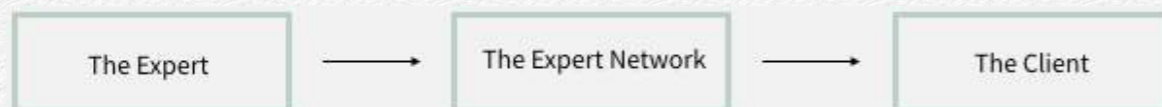
\*\*\*

**Is this also true for expert calls?** Let's look at a basic scenario: A client uses an expert network to recruit experts for the purposes of providing expert consultations. For simplicity, all parties are based in the EU.

The definition of personal data under GDPR is rather broad. It includes any information that can be used to identify a natural

person, no matter if it needs to be combined with other data. Career history for example qualifies as personal data, even if a person's name has been removed from the resumé.

If we would map the flow of personal data related to experts engaged by the expert networks to provide consultations to clients, it would look like this:



- The *expert* is the *data subject*, the natural person whose data is being collected and processed.
- The *expert network* determines the purpose and the means of the processing of the personal data, and hence acts as *data controller*.

We will soon discuss what it means to be a data controller and which responsibilities it entails, but first we will look at the role of the client.

\*\*\*



Source: European Commission

# 2

## CONDUCTING EXPERT CALLS

- *The role of the client*



---

**In the previous chapter**, we discussed which role the expert network takes in the processing of personal data when recruiting experts for expert calls.

The expert network generally determines the purposes and means of processing of personal data when recruiting experts, and hence act as a data controller (if you need a recap on the definitions under GDPR, go back to chapter one).

The expert, on the other hand, is the natural person whose data is being processed, and hence takes the role of a data subject.

\*\*\*

### **But where does this leave the client?**

From a first look at the definitions, it's easy to think that the client is just a recipient.

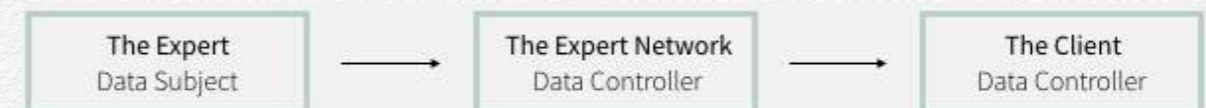
But is it true that the client merely accesses anonymized expert profiles, and doesn't perform any processing activities on its own? Or does the client take the role of a data processor, acting on behalf of the expert network?

### **Let's revisit the definitions**

A data processor is *"a natural or legal person which processes personal data on behalf of the controller"*.

In order for the client to act as a data processor, it would need to process the data on behalf of, and as instructed by, the expert network. Most clients would disagree, and claim that it's rather the expert network that is acting on the client's behalf when sourcing experts.

But if the client does not take the role of a data processor, which role does it take? Well, as soon as the client accesses personal data related to an expert and starts processing it for its own purposes, it becomes a data controller in its own right.



---

### WHAT DOES THIS MEAN FOR THE CLIENT?

In practice, this basically means that when an expert's career history is downloaded on a local server, or any information that can be used to identify that person is compiled in a spreadsheet, the client is obliged to take full data controller responsibility for that processing.

\*\*\*

### Joint or independent controllers?

GDPR introduces the concept of joint-controllers, when two or more controllers jointly determine the purposes and means of processing.

That is not the case in this situation though: instead the expert network and the client act as *separate and independent controllers* and each party is responsible for its own processing of the data, and for fulfilling the requirements imposed by the GDPR.

### A robust plan for GDPR compliance is often missing

Despite their best intentions, many clients of expert calls do not have proper processes in place to ensure the protection of personal data when conducting expert calls. Instead, their main focus is on overall project confidentiality and compliance.

In the Inex One *Expert Network Usage Survey 2019*, conducted in January 2019, most clients agreed that they still have work to do related to GDPR.

#### *The role of the organization:*

- 60% of respondents said that their organizations have not yet defined their role under GDPR when handling personal data in relation to expert calls.
- 26% of respondents identify their organization as data processors, and only 14% as data controllers.

---

*The strategy for GDPR compliance:*

- 71% of respondents say that they leave full responsibility of GDPR compliance with the expert networks.
- 23% of respondents say that they have adapted and documented their processes.
- 6% of respondents say that they have changed the way they source experts because of GDPR.

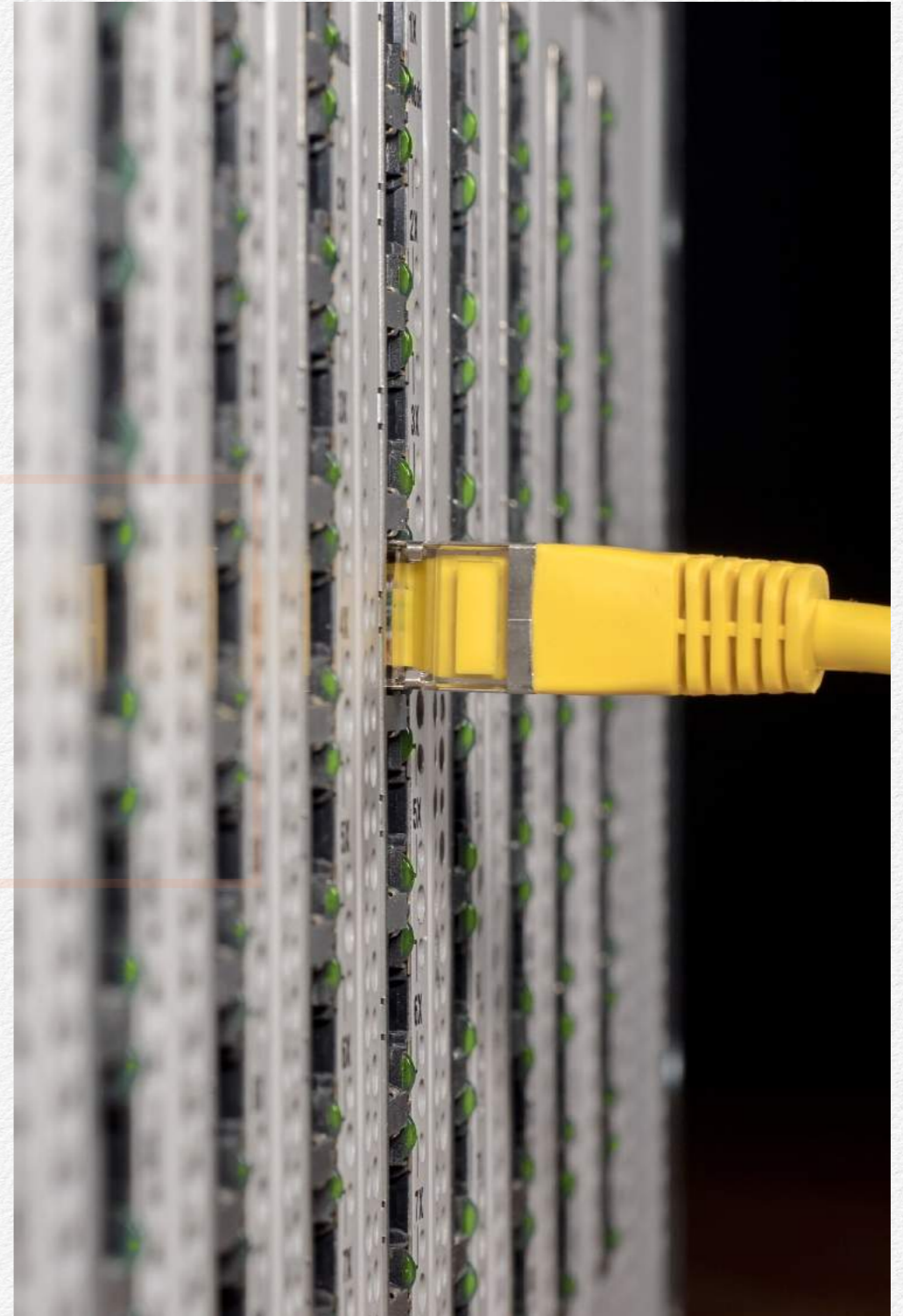
\*\*\*

So what does it mean to be a data controller, and which responsibilities does a data controller have? Read more in the next chapter.

# 3

## BEING A DATA CONTROLLER

- *Obligations and responsibilities*



---

**The role of the data controller** is connected to a list of obligations and responsibilities. In this chapter, we will take a closer look at a few of them: legal basis for processing, data storage limitation and the individual's right to erasure.

\*\*\*

### **Legal basis for processing: Consent vs. legitimate interest**

A data controller needs to define a legal basis for each processing activity it's performing. For an expert network, this means the data processing taking place in the sourcing stage of a project, as well as when an expert has been contracted.

While the GDPR defines six different legal bases that organizations can gather personal data under, *consent* and *legitimate interest* are the ones most often discussed in relation to recruitment.

**Consent means that the data subject** has agreed to the processing. Under the GDPR, a consent must be freely given and specific to each processing activity. General consent that

covers multiple processing activities or implied consent by pre-ticked boxes are not sufficient.



### **CHECKLIST FOR CONSENT UNDER GDPR**

Consent under GDPR means giving the data subject a real choice and control over how its data is handled.

Here is a checklist to get you started:

- Ask the Data Subject to positively opt-in
- Don't use pre-ticked boxes
- Use clear language that's easy to understand
- Specify the purpose and the means of the processing
- Ask for consent for each separate processing activity

---

**Legitimate interest means that the organization** can prove that it has a legitimate interest to perform the processing, and that such interests are not overridden by the interests or fundamental rights of the data subject.

Legitimate interest is the most flexible of the legal bases, but it can't mechanistically be used to motivate just any kind of processing. The data controller needs to be able to demonstrate that it's using the data subject's personal data in a way that he or she would reasonably expect, and where there is a valid justification for the data being processed.

Legitimate interest can be an appropriate lawful basis when sourcing experts for expert calls. It's important to note however, that only such personal data that the team needs in order to contact or evaluate the expert should be collected. Irrelevant data, or data that includes sensitive information (like race and ethnic origin, religious or political beliefs and disability or genetic information) should generally not be collected as part of the expert sourcing process.

\*\*\*

No matter if the expert network relies on consent, legitimate interest or one of the other legal bases, it should be clearly stated in its privacy statement or privacy policy.

### WHEN DOES LEGITIMATE INTEREST APPLY?

Legitimate interest is the most flexible of the legal bases under GDPR, but in practice it can be difficult to figure out if it's appropriate to a specific processing activity.

In general, you can rely on legitimate interest when you use people's data in ways that:

- They would reasonably expect you to
- Have minimal privacy impact
- Have a compelling justification



---

## Publicly available data

Anyone who has worked with recruiting experts for expert calls knows that it's a task performed under constant time pressure. Deadlines are tight, and you want to get to the expert before any of your competitors do.

Every now and then, an expert network will present an expert profile to a client before that expert has been contracted. Or the recruiter will come across an interesting expert profile and save it on a hard drive or in an internal system just in case it will become relevant in another project.

In these cases, the expert network will collect personal data from publicly available sources, but process it for its own purposes. As soon as that processing starts, the expert network gets the status (and responsibilities) of a data controller.

\*\*\*

**A legal basis for processing is always required**, regardless of where or how the personal data was first collected. If consent has not been obtained directly from the data subject, the data

controller is responsible to get in touch with the data subject to provide information about the processing.

The information should contain details about which purposes the data is processed for, the legal basis for the processing, the data retention period, and other relevant information.

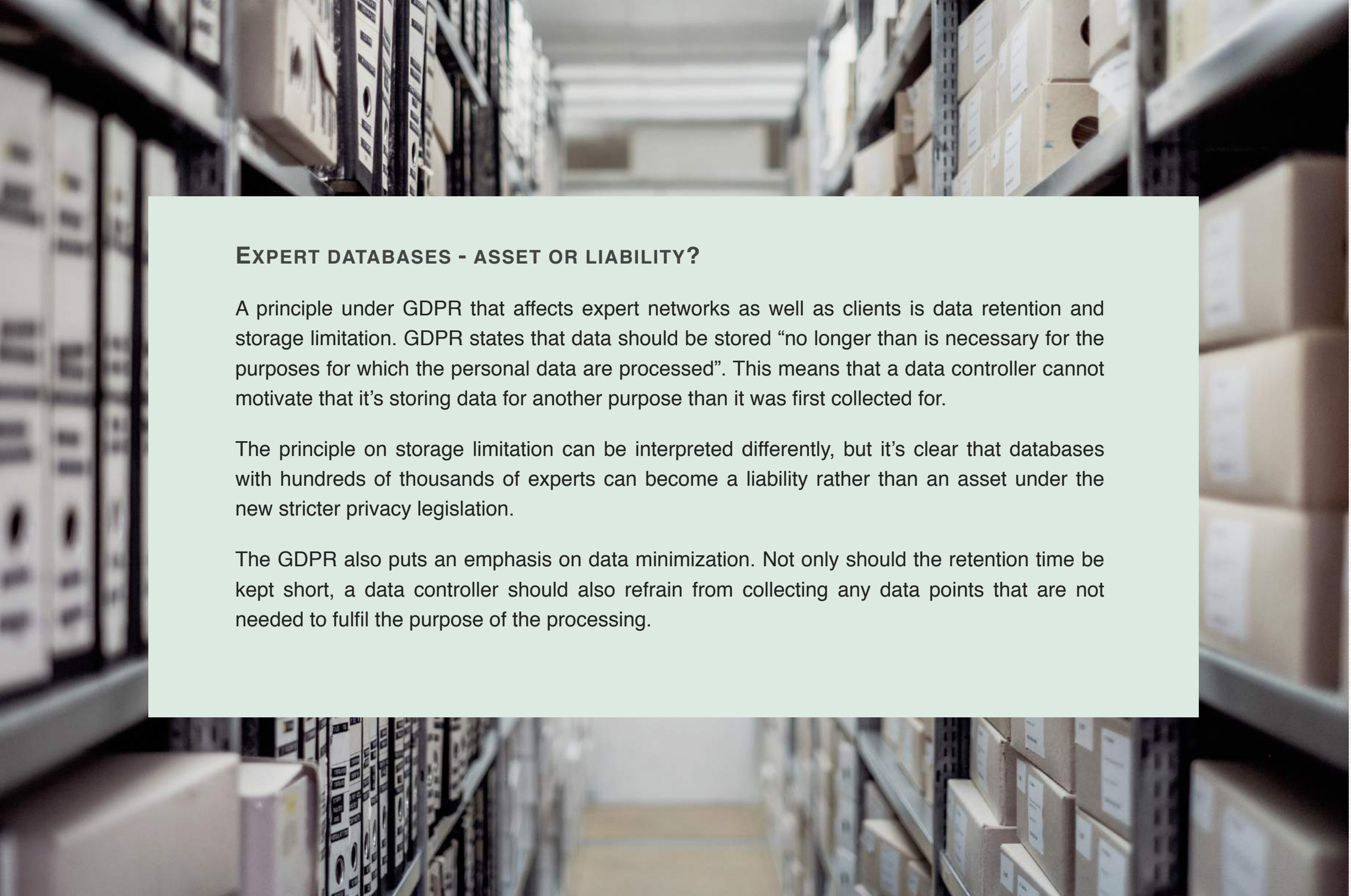
The expert network must contact the (prospective) expert in a reasonable period after obtaining the personal data, but at the latest within one month.

\*\*\*

## The principle of 'Storage Limitation'

According to the principle of storage limitation, a data controller should not store personal data "longer than is necessary for the purposes for which the personal data are processed".

For a client, this means that when a project has ended and the expert data is not needed anymore, it should be deleted or anonymized. And this requirement does not only concern directly identifiable personal data like name and phone number, but also indirectly identifiable data like career history.



### **EXPERT DATABASES - ASSET OR LIABILITY?**

A principle under GDPR that affects expert networks as well as clients is data retention and storage limitation. GDPR states that data should be stored “no longer than is necessary for the purposes for which the personal data are processed”. This means that a data controller cannot motivate that it’s storing data for another purpose than it was first collected for.

The principle on storage limitation can be interpreted differently, but it’s clear that databases with hundreds of thousands of experts can become a liability rather than an asset under the new stricter privacy legislation.

The GDPR also puts an emphasis on data minimization. Not only should the retention time be kept short, a data controller should also refrain from collecting any data points that are not needed to fulfil the purpose of the processing.

---

Most clients find it hard to live up to this requirement. The way that sourcing of experts is handled, personal data quickly spreads from email servers to spreadsheets, and then on to notepads, word documents and other systems.

Even when an organization has internal processes in place around storage limitation with regards to personal data, these are not always followed by the individual employees whose focus is on the organization's core business.

\*\*\*

### **The individual's right to erasure**

The GDPR has given individuals certain rights to empower them to take control of how their personal data is being processed. Out of the different rights defined in the law, the *"right to erasure"* or *"right to be forgotten"* is probably the most well known.

**The right to erasure means** that individuals have the right to have their personal data erased:

- if it's no longer necessary for the purpose it was originally collected or processed for (e.g. when a project has finished)
- if the original consent is withdrawn, or
- if you as the data controller rely on legitimate interest as your basis for processing and the individual objects to the processing.

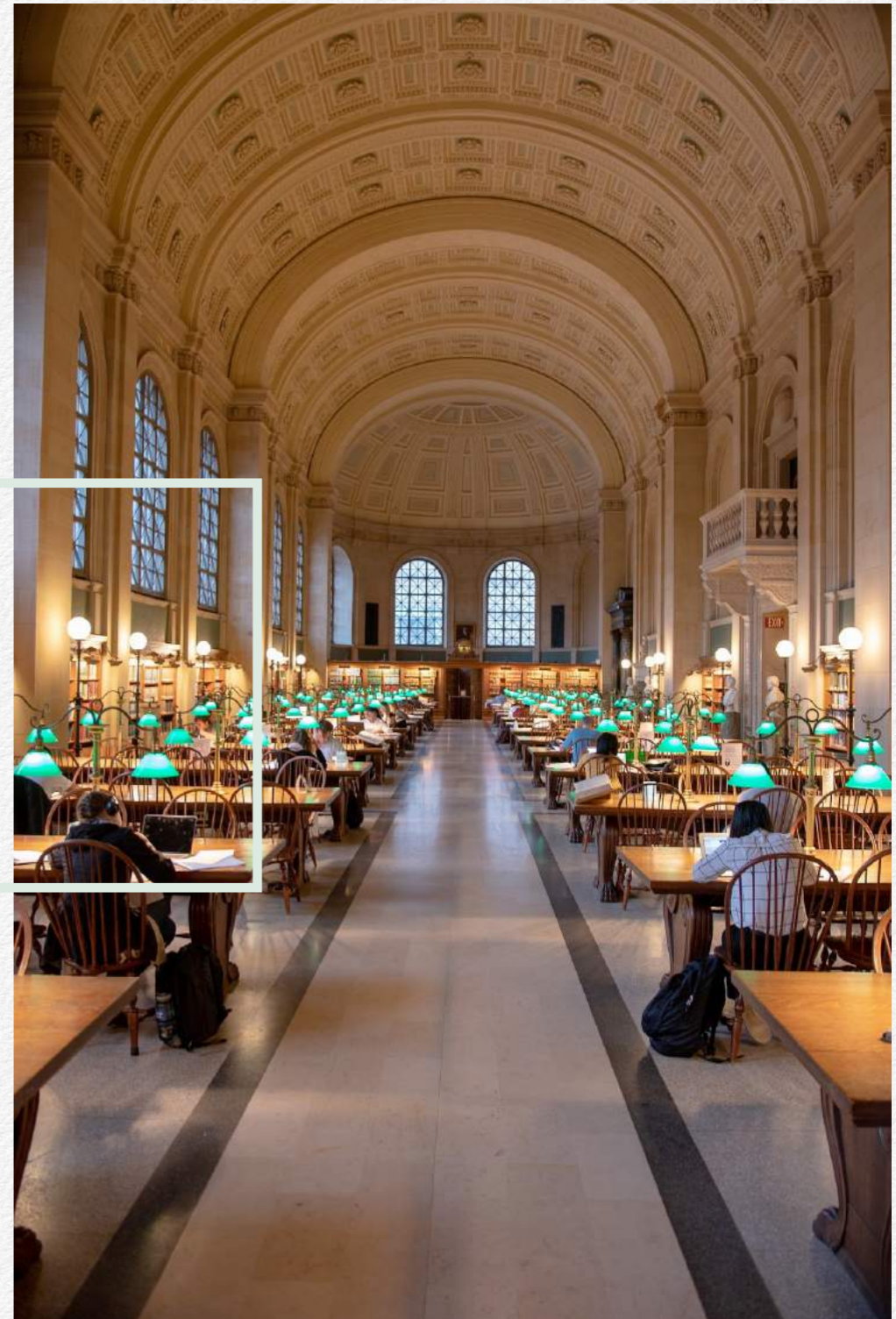
If a request for erasure is made by an individual to a data controller, the data controller has one month to respond and act on the request. In the setting of expert calls, this means that a client and/or expert network must identify and delete all personal data related to a particular expert. In practice, old email conversation, as well as text files and spreadsheets on hard drives, local servers, cloud services should be deleted or anonymized.

**These kinds of requests from individuals can easily become an administrative nightmare**, as many companies don't have appropriate processes and methods in place to identify and delete personal data related to expert calls.

# 4

## BEING A DATA PROCESSOR

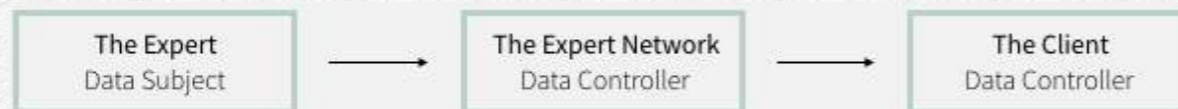
- *Obligations and responsibilities*



---

So far, we have looked at the roles and responsibilities of the expert networks and clients when processing expert personal data.

To recap, we landed in that the *expert* is a *data subject*, and the *expert network* and the *client* act as *separate and independent data controllers* when processing personal data in relation to expert calls.



But the supply chain is rarely this clean. What happens if one or several of the parties engage with a data processor? Which responsibilities do data processors have, and to which extent is the controller responsible for the processing performed by its processors?

\*\*\*

## Data processors used in relation to expert calls

In today's connected world, most data controllers use data processors to assist them in the processing of personal data.

- Most expert networks use some sort of *Recruitment Management System* to manage expert profiles.
- *Email* is used as the primary tool of communication between the expert network and the expert, as well as between the expert network and the client.
- The client team often compiles expert profiles in a *spreadsheet* to distribute to colleagues in the internal team.
- The expert call itself often takes place in a third party *phone conferencing system*.

All of these systems and services '*process personal data on behalf of the controller*' and hence act as *data processors*.

\*\*\*

## THE RESPONSIBILITIES OF THE DATA PROCESSOR

A data processor has several responsibilities to the data controller it is processing data on behalf of.

Amongst other things, the data processor should:

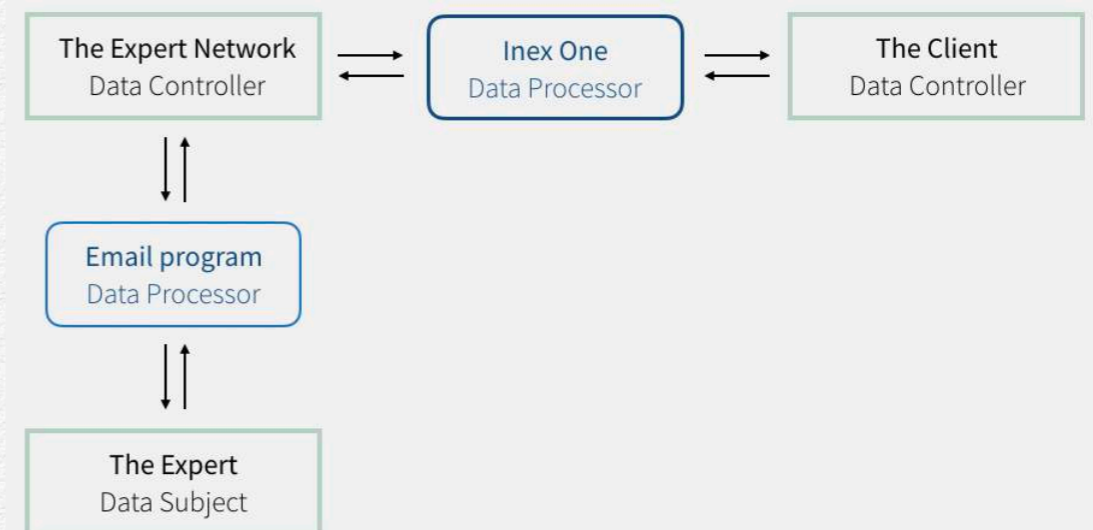
- Only act on behalf of, and as instructed by, the data controller.
- Implement appropriate technical and organizational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject.
- Not engage another processor (sub-processor) without prior authorization of the controller.



## Inex One takes the role of a data processor

Inex One replaces the need of using an email program to communicate with expert networks, and the need of using MS Excel or other softwares to compile and administer expert profiles.

We act as a *data processor* in relation to both the expert network and the client, just the way an email program or a Recruitment Management System is.



---

A data processor is responsible to make sure that the processing it's undertaking meets the requirement of the GDPR, but it's up to the controller to check that their processors can give sufficient guarantees that they will protect data subjects' rights.

\*\*\*

## Data Processing Agreements

Whenever a data processor is processing data on behalf of a data controller, there should be a written contract in place to stipulate the obligations, responsibilities and liabilities of the parties involved.

If a data processor uses another data processor (i.e. a sub-processor) to assist in the processing of personal data for the controller, it needs to have a written contract in place with that sub-processor.

Such a contract is referred to as a Data Processing Agreement (DPA). It is the responsibility of the data controller to sign a DPA with the data processor that is processing data on its behalf.

It's important to remember that a data processor often has its own data controller responsibilities for data that it's not processing on behalf of the data controller, for example data on its employees.

### CHECKLIST: DATA PROCESSING AGREEMENTS

The Data Processing Agreement should set out the details of the processing, including:

- The subject-matter of the processing
- The duration of the processing
- The nature and the purpose of the processing
- The type of personal data involved
- The categories of data subject
- The controller's obligations and rights



# 5

## GDPR IS A GLOBAL CONCERN



## GDPR is a global concern

Investment research is a global market, and the search for knowledge and expertise goes across national borders. When conducting expert calls, it's not unusual that the client, the expert network and the expert are based in three different parts of the world.

\*\*\*

## What if only one party is based within the EU?

The GDPR is a regulation on the data protection and privacy for all individuals within the EU/EEA, but it also addresses the export of personal data outside of the EU/EEA areas.

The GDPR applies to the processing of personal data:

- by a controller or processor based in the Union, regardless of whether the processing takes place in the Union or not.
- by a controller or processor *not* established in the Union, if the data subject is in the EU and the processing activities are

related to the offering of goods or services to such data subject.

Related to expert calls, this means that the GDPR applies:

- if the expert is based in the EU/EEA, regardless of where the expert network and the client are based.
- if the client or expert network are based in the EU/EEA, regardless of where the expert is based.

### CHECKLIST: IS MY ORGANIZATION IMPACTED?

If your answer is “yes” to any of the following questions, your organization most likely needs to comply with the GDPR:

- Is your organization based in the EU/EEA?
- Does your organization manage personal data of EU residents, such as experts engaged in expert calls?



---

## International transfers

The GDPR restricts the transfer of personal data to countries outside of the EU/EEA. The restrictions apply to controller-to-controller transfers, as well as controller-to-processor transfers, or processor-to-sub-processor transfers.

As soon as an expert network established in the EU works with a client outside of the EU/EEA and shares an expert profile with the client, the expert network must take ‘appropriate protection measures’ to ensure adequate level of data protection. In practice, this means that the two companies should sign Standard Contractual Clauses as an addition to the Data Processing Agreement (read more about Data Processing Agreements on page 20).



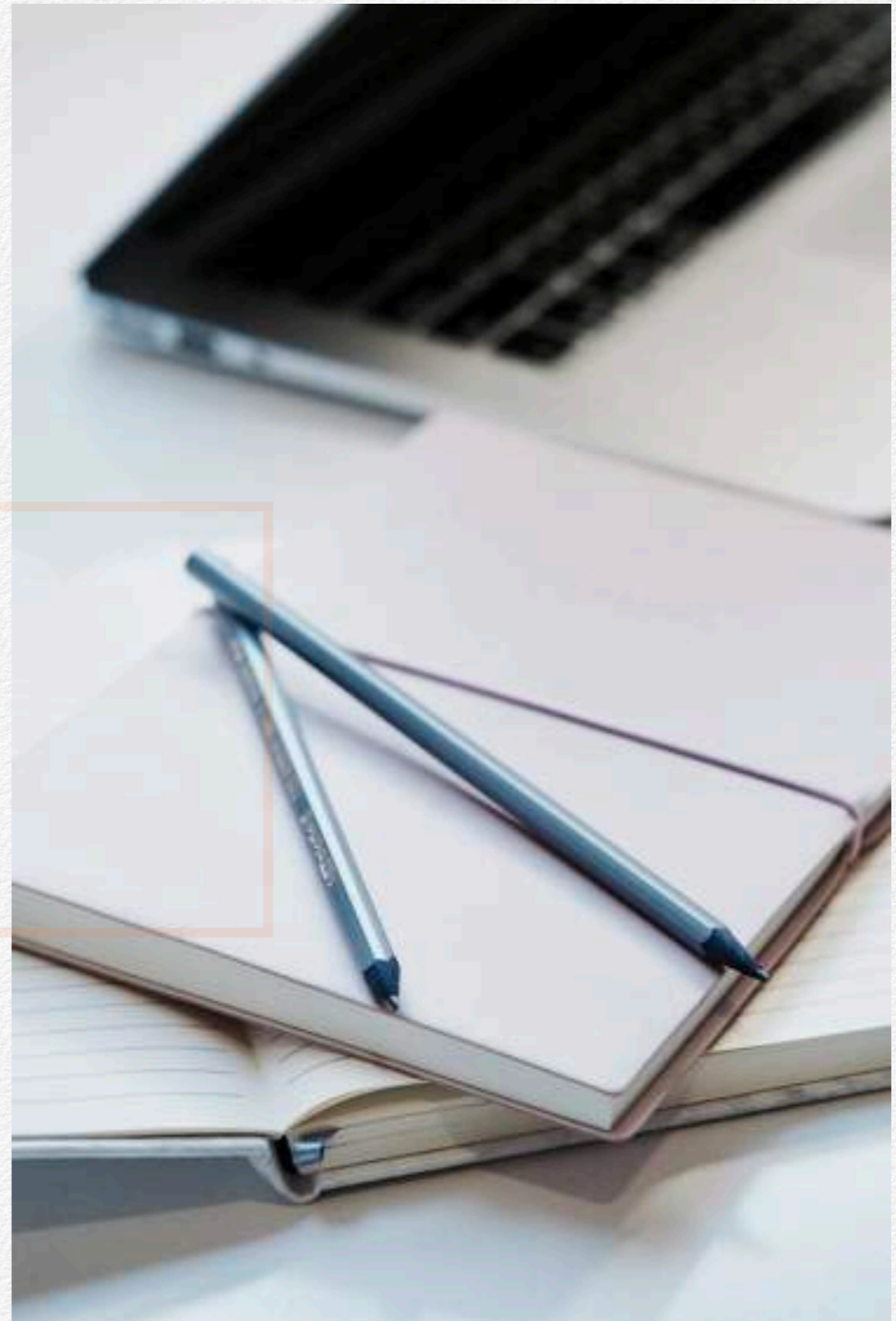
### DID YOU KNOW?

If the expert (data subject) is based in the EU/EEA, the expert network (the data controller) needs to comply with GDPR regardless of where it's based.

# 6

## PUTTING PRIVACY FIRST

- *How Inex One supports your GDPR compliance efforts*



---

**At Inex One, we understand that every organization is unique,** and that every customer has different compliance needs.

Whatever your level of concern about GDPR, the Inex One Expert Management System is here to support you in your data protection efforts.

\*\*\*

### **Putting privacy first**

When using Inex One, there is no need to compile and distribute information about experts in spreadsheets to colleagues, or to use email to communicate. Instead all data is processed within a closed and encrypted ecosystem.

Inex One was built according to the principles of privacy by design, and has a built-in functionality for storage limitation.

Our strict data retention schedules ensure that you do not hold expert personal data longer than necessary, and if you would receive a request for erasure for data that has not already been

anonymized, we have robust processes in place to have it deleted for you.



### **DID YOU KNOW?**

As a client of expert calls, it's crucial to work with partners who adhere to the requirements of the GDPR.

A data breach or a lawsuit where an expert network is found to misuse personal data can severely damage the brand of its clients.

Our general advice is to ask your expert network how they handle the requirements of the GDPR, and which responsibility they take in the processing of expert personal data.

Which processes do they have in place to keep expert database up to date, and which legal basis are they relying on when processing personal data?

## ABOUT INEX ONE

Inex One is a cloud-based Expert Management System (EMS) that helps professional firms manage their expert interactions in one single platform.

Inex One makes it easier than ever before to track costs, consumption and time spent with each research provider.

If you want to know more about how the Inex One Expert Management System can change the way you manage expert calls visit [www.inex.one](http://www.inex.one) or get in touch at [info@inex.one](mailto:info@inex.one).

