The Market Researcher's Friendly Guide To Data Security & Compliance

TAKE NOTE

Introduction

Welcome to your friendly guide to data security & compliance, written for all you wonderful researchers out there.

And, thank you for selecting this guide. We know the topic can be a little bit on the dry side, so we're hoping to deliver you the jaffa cake version, not the digestive. Our aim is to provide you with the essential information in a user-friendly format, that's easy to digest and hopefully won't bore you to tears.

Disclaimer

We have written this guide to provide useful information for Market Researchers who are invested in the security of the data they collect. However, this guide should not be treated as legal or compliance advice. You should seek professional support and advice where needed.

The information contained in this document was correct at the time of writing, however regulations and best practice recommendations do change.

You ready? Let's get started.

Contents

Our Qualifications for Producing this Guide

First up. Why should you listen to us anyway?

Good question. We are after all, first and foremost, a transcription company.

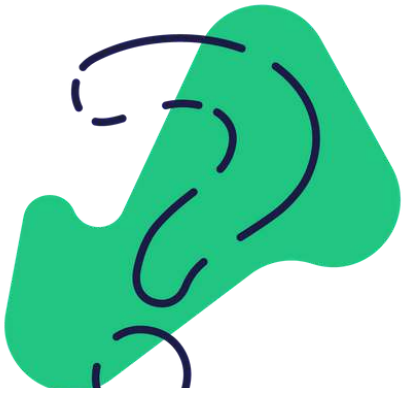
Clients trust us to keep their data safe and secure and we take that obligation pretty seriously. That means that we make it our business to keep up with not only the regulations but also best practice when it comes to handling, managing and storing personal, sensitive and confidential information.

Meet Owen, our Head of Compliance.

We think we're quite unique for a supplier of our size to have invested in a Head of Compliance, but we're committed to ensuring we don't let any of our clients down and Owen is an integral part of that promise (we told you we take data security seriously).

We have experience at working with a broad range of clients from the largest global agencies through to the specialist boutique suppliers and everything in between. Our transcription services cover a whole host of qualitative methodologies including focus groups, IDIs & User Testing, as well as working with audio and video content.

Why you should care about data security & compliance



The fact that you're reading this guide is a good indication that you already recognise the importance of data security, so we won't dwell too much on this point.

When it comes to data security & compliance there are some legal requirements that must be adhered to, which are obviously vital for businesses to follow.

However, in addition, consideration has to be given to the reputation of the research industry as a whole. Research needs participants and therefore we need to do everything we can to protect that relationship and deliver on the promise to keep their information safe.

Research participants open up and share their thoughts, feelings, as well as personal information to help generate insights that are used to guide decision making - that information exchange is built on trust. Without trust, Market Research becomes a whole lot more challenging.

Data security considerations for researchers

Why is it important?

In Market Research a whole myriad of information and different types of data is handled. Some of the data types you'll likely to come into contact with are:

Sensitive - Within the broad category of personal data, there is information that is deemed particularly sensitive. Due to the nature of research, this is also information that may often be collected and includes race, ethnicity, sexual orientation, health data, as well as religious beliefs and political opinions.

Whether you find yourself dealing with one, or all these data types, you will want to keep the data secure and prevent it from falling into the wrong hands.

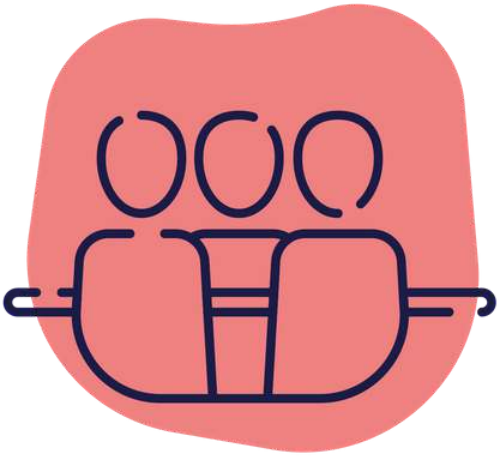
Personally Identifiable Information (PII) - this is information that could potentially identify a specific individual. Some information, such as full name or passport number, is enough to identify an individual on its own. In other cases, separate pieces of data may need to be pieced together to identify someone at an individual level.

Confidential - Market Research provides unique insight which helps organisations to make decisions. In light of this, often the themes and topics that form the research mean that confidential information is involved. Examples include; focus groups on innovative solutions, feedback on prototypes and testing of potential marketing messages.

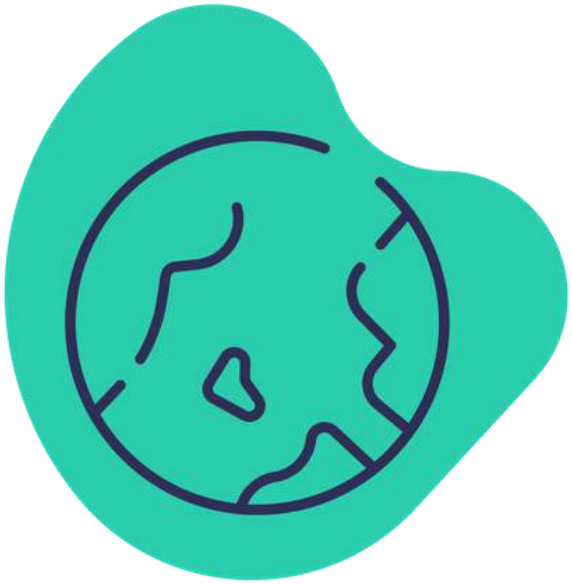
Participant-led considerations

Specific groups

As well as the general considerations you need to apply to all participants, there are particular groups that are subject to additional scrutiny, such as children.



Their data is often classified as particularly sensitive and there are other specific research guidelines in place to ensure individuals are approached and interacted with appropriately.



Location

When conducting research in different countries there are elements such as language, culture and timezones that can all pose unique challenges. In addition, different locations can often have different rules and regulations in place. It is often not as simple as applying the rules you would in the UK to participants elsewhere in the world.

Make sure you know of any location-specific data protection and privacy laws that you need to adhere to.

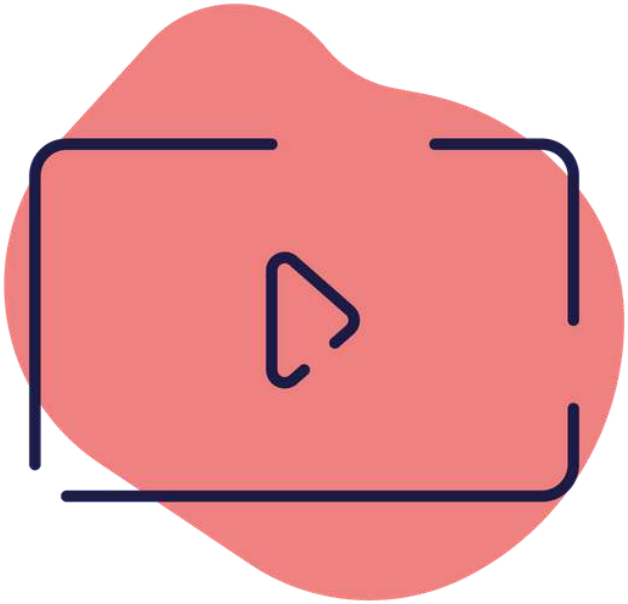
Project design & methodology

When you are designing a research project, you'll have a clear idea of who the participants will be and the subject of the research. This will help you plan for the type of data you will collect, whether it includes personal information and how sensitive and confidential the information is. What is more challenging to know is how participants will respond and what they will say.

Alongside identifying the type of data you are requesting, you also have to consider data that's collected unintentionally, such as when respondents mention personal or sensitive details in open-ended questions or comments.

Video & Audio

The use of video has rapidly accelerated during the pandemic as people looked for ways to conduct research that would have previously happened in a face-to-face environment. Regardless of what the respondents might talk about, their voice through audio and their face via video, could be classed as personal data.



Operational information

In addition to the information you require to deliver on the goals of the research, you'll also inevitably require other information to help with the running of the research project. This may include, but is not limited to:

- Name & contact details
- Bank details or address for an incentive payment
- IP address for deduplication of survey responses

Much of this data does not form part of the project deliverable, but is essential and needs careful consideration in terms of how it is collected, transferred and stored. It is also likely that this information will be required for a shorter period of time than the final results of the project.

You need to consider all of the data that forms a project, not just the information you explicitly ask for.

Best Practice

Although there are certain instances where you may need to be more diligent with data security, a good rule of thumb is to treat all your data with the highest level of care, that way, you can ensure you don't inadvertently fall foul of the rules and put any information at unnecessary risk.

Here are some basic principles that will help you to establish best practices for collecting, handling and storing data.

- Only collecting/keeping what's needed
- Only giving access to those who need it
- Deleting data after a certain amount of time
- Be clear, open & transparent
- Opt-in not opt-out

Only collecting/keeping what's needed

When running projects it can be tempting to ask for as much information as possible. You never know what insights it might reveal, right?

A good discipline though is to only collect the information you need, particularly when it comes to personal or sensitive data - this makes for a better user experience too.

Only giving access to those who need it

Despite the trustworthiness of your colleagues, accidents do happen.

You can minimise the risk of human error by reducing the number of people who have access to any data to start with.

Technology can be your friend in these cases to help lock down access, ring-fence data and make it harder not only for hackers but for pesky human error to occur.

Deleting data after a certain amount of time

I think we can all be guilty of the 'just in case' mentality when it comes to information. Just a quick glance into most people's email boxes or computer drives will attest to that. It's good to review what information needs to be kept and for how long. You may also find that you can remove some personal data whilst keeping other results intact, therefore minimizing any risk.

Be clear, open & transparent

If you go through the stages above it's easy to be clear, open and transparent with your participants. This gives people all the information needed to ensure that they can make an informed decision about taking part in any research, and gives them clarity on where their data will go, what it will be used for, and how long it will be kept for. You can also give them the relevant details if they decide they want their data removed at a later date.

Opt-in, not opt-out

Some opt-ins leave you so confused about whether you've actually opted in or out - not great from a user perspective. No-one likes to feel that they're been tricked into something.

Make any opt-in messages super-clear, at least then you'll know that participants really want to be involved.

How to reduce risk of a data breach

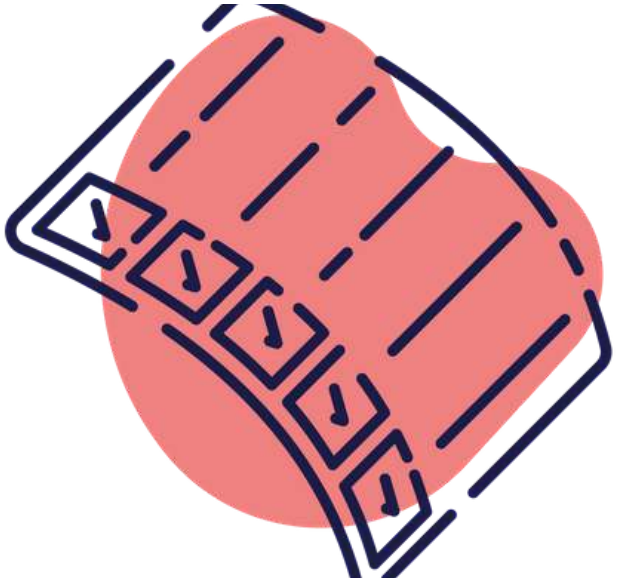
Conduct an audit

A good first step is to conduct an audit to understand what data you have already, as well as information you're likely to collect in the future. Your organisation will have conducted this type of audit as part of the GDPR, but it's good practice to revisit periodically.

Anyone working on a project should have a good understanding of:

- The type of information been collected
- How data should be collected, managed and stored
- Who has access to the data
- How long the data should be kept for
- Who is responsible for deleting data when required

Processes, policies & training



Processes and procedures may have many of us rolling our eyes (except for Owen of course), but they are essential in ensuring we are compliant. They provide the structure and workflows needed to minimise any risk and provide a framework to deal with any breaches quickly and efficiently.

All too often though, policies and procedures are put in place but the training to accompany them is lacking, or they're not adhered to as rigidly as they should be. For example, maybe a client emails over a list containing some personal details rather than using the secure channels that have been put in place, but you let it go, just this time. We'll be discussing human error in more detail shortly.

You want to establish a culture where data security is part of the everyday language, from the initial induction process, all the way through to when someone leaves the organisation. You want people to feel comfortable raising any concerns and reporting any issues that need to be investigated.

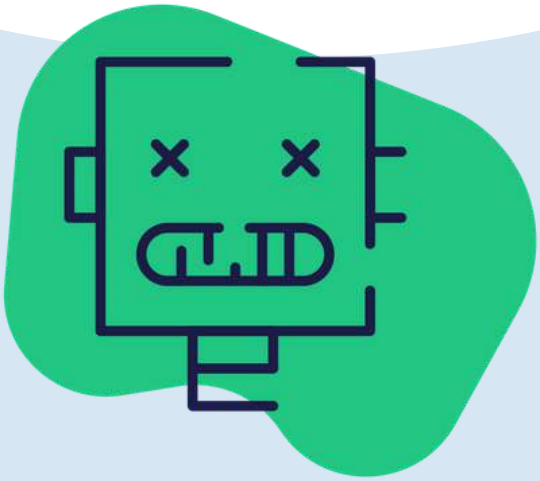
Utilising technology

Technology can be a great support when it comes to security and compliance but it also needs processes in place to ensure we're benefitting from the capabilities on offer.

This can include; making sure we install the latest updates that are designed to counteract the latest security threats, using secure portals and encryption for data transfer and storage, and accessing information through secure means such as virtual private networks (VPN).

And don’t even get us started on passwords and enabling two-factor authentication (2FA)

More on technology later.



Keeping your data safe

According to CybSafe, human error caused a whopping 90% of cyber data breaches in 2019[1].

Minimising human error

Although, as we've mentioned, technology can play a useful role, it can't eliminate all risk. As individuals, we need to stay vigilant to threats. Even when we're using all the technology available to us correctly, there is still a chance of human error occurring - and potentially, an even greater risk if we become too complacent that technology can do all the work for us.

I'm sure you'll have received a phishing email in the past. Some are more obvious than others, that Nigerian prince gets about! However, there are some scarily convincing versions that also do the rounds. They may look like they come from your bank or another service you are signed up with.

Potentially less well known, is the fact that businesses can also be hit with phishing emails that look like they've come from someone in your organisation. Not only do the emails look realistic, but they may also be written in the style and tone you expect.

Good policies also have a role to play here. By setting out clear processes for sharing sensitive and confidential information you can mitigate the impact of a phishing incident. If in doubt, pick up the phone or use another type of communication to double-check. This really is one of those 'better safe than sorry' scenarios.

Here are some other examples of human error to watch out for:

- Accidentally downloading a malware-infected attachment
- Sending data via insecure means such as email or accidentally sending information to the wrong person (recall, recall!)
- Revealing information through social engineering
- Leaving sensitive or confidential information unattended in a non-secure environment - yep, that quick stop for a coffee or leaving a bag on a train

And everyone's favourite - Passwords!

- Weak passwords (123456, password)
- Reusing passwords
- Writing down passwords

You get the point, passwords can be a problem. It's vital to consider how the risks associated with passwords can be reduced. This could include a well-devised password policy, or potentially the implementation of a password manager in the right circumstances.

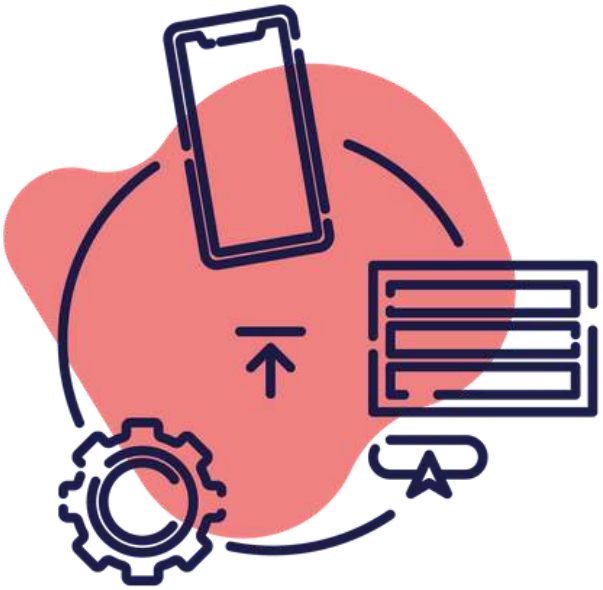
How technology can help

As we've been flung into more flexible working environments, locations and hours, there are some security-related aspects of home working that need to be considered.

Many of these also apply when we're on the move and making use of the connected world.

When we're tucked up in our offices there are layers of security to protect our servers, networks and individual machines.

As the lines become increasingly blurred, it's easy to pick up a personal device to carry out work tasks or jump on a public wifi network to send a quick email. However, in doing so we are increasing the risk of a data breach.

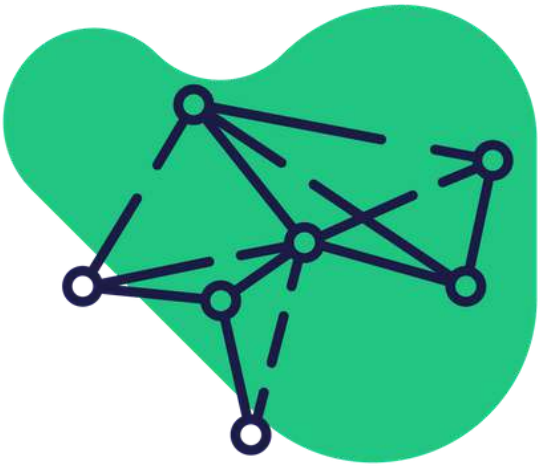


Layers of security when accompanied by the right processes and training can help to mitigate the risk and ensure you feel confident in what you should, and shouldn't be doing. Here are just some areas to be aware of when dealing with data.

Encryption

Encryption basically makes it possible for only authorised parties to decipher any given information. Encryption is commonplace across the internet. When you use a https site, the ones with the reassuring padlock, it means any data you input is being encrypted.

You should stick to using encrypted methods of transferring data as well as storing it.



Virtual Private Networks (VPN)

You may already be using a VPN and have this provided by your company. You can also sign up for a VPN for personal use.

A VPN provides a secure connection between you and the internet. This can be particularly beneficial if you find yourself using public wifi. VPNs have some other uses, some of which aren't exactly legal, so make sure you're using them for the right reasons.

Two-factor authentication

Many sites and services will offer you a 2-factor authentication option (2FA). This means you need two ‘factors’ to gain access. Typically alongside a known piece of information, such as a password, you also need to use another method. This could be something in your possession, like a text to your phone, or biometric identifiers (fingerprints, facial or voice recognition).

It will provide an additional layer of security, but it’s often presented as optional, rather than mandatory. As a concept, it can put some people off as it’s an extra step in a process, but it is usually quick and easy to set up.

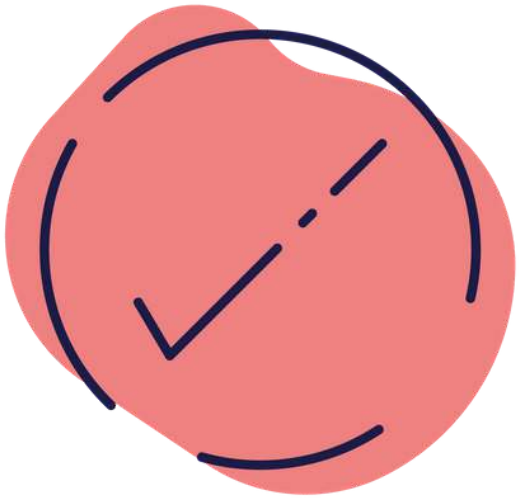
Keeping up to date with updates

If you're like us, your heart sinks a little every time you get ‘an update is available’ message on a device. The update itself isn't really the problem, but it always seems to pop up at an inconvenient time and it gives you no reliable indication of how long it might take - it seems to range from anywhere between a few seconds to hours!

Despite the irritation, the updates are extremely important. They may include new or enhanced features, but the key reason to apply them, in a timely fashion, is that often they contain security fixes.

When vulnerabilities are detected ‘patches’ are delivered through updates to resolve the issues found and to keep your data safe.

So, next time you start to hover over the ‘remind me later’ option, maybe think twice.



Pseudonymisation and anonymisation

Pseudonymisation is a security technique often used to protect data subjects so they can't be identified without the means to reverse the pseudonymisation. You'll likely have seen this in action on a research project where personal data such as names is replaced by an ID or reference number. You can only tie the data back to the individual if you have access to the relevant information. Although, it's important to remember that this process doesn't change the nature of the data and it still falls within the scope of GDPR.

Anonymous data on the other hand is not considered to be personal data at all and so is outside the scope of GDPR, which has huge compliance benefits. Anonymised data does not relate to an identified or identifiable person and therefore poses no risk to individuals. It makes sense to anonymise data wherever you can, however, make sure you're clear that the information is truly anonymous and not just using pseudonymisation.

GDPR

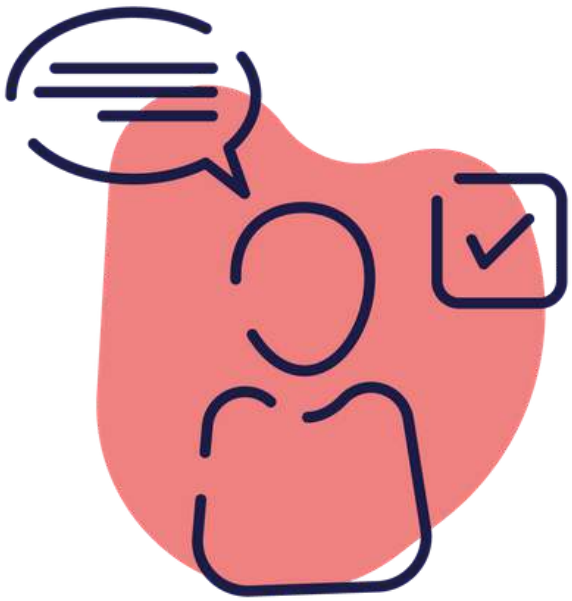
What is GDPR?

It's been around for a while, but let's do a quick recap.
The General Data Protection Regulation (EU) 2016/679 is an EU regulation that took effect way back on 25 May 2018.

It applies directly in all EEA countries and deals with how personal data is processed. At the heart of the GDPR are six key data protection principles, together with the concept of accountability, and expanded rights for data subjects.

Why is it important?

Personal data goes one step beyond PII and looks at data relating to those identifiable individuals, which is quite a broad scope. Of course, personal data isn't the only thing you need to consider when you're thinking about information security, but the statutory obligations placed on organisations by the GDPR mean that it's likely to be one of your biggest compliance burdens, and the penalties for getting it wrong can be steep - just ask Google (fined €50m), British Airways (fined €22m) and H&M (fined €35m).



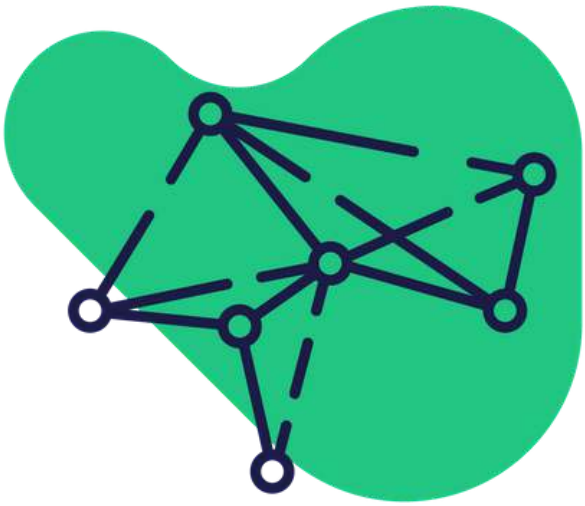
Many of the best practices we've talked about throughout this guide (like only collecting data that you need for your purpose, for example), become legal requirements under the GDPR when you're dealing with personal data. It's important to make sure that you have a good understanding of your obligations as well as having the right processes and procedures in place to meet those obligations.

Implications for Market Research

The implications of GDPR on research (and for many areas of business) are wide and far-reaching. It impacts how you connect with participants, what information you hold about them and what details you need to provide them in return. It also gives participants greater control over how their information is used and their right to be forgotten.

GDPR provides some interesting challenges for market research in particular, such as when a client or brand wants to remain anonymous. Whether you are a fan or not, it does provide greater transparency for individuals and instils best practices in (most) businesses. As we've mentioned, trust is an important factor in engaging participants and GDPR helps to nurture this.

We mentioned that it's a really good idea to be clear, open and transparent when you're dealing with data and that concept is well aligned with the first data protection principle in the GDPR, which says that personal data must be processed "lawfully, fairly and in a transparent manner". If you set out to embed that principle in your organisation's culture, you should find that compliance with the other data protection principles, and the GDPR as a whole, follows on naturally.



Implications due to Brexit

For European research

GDPR remains in place for the European Union so where you are conducting research across those countries you need to abide by the regulations.

If you're part of a UK organisation that doesn't have an EU establishment, you'll also need to consider whether you need a GDPR EU representative, in relation to any processing that falls under EU GDPR.

For UK research

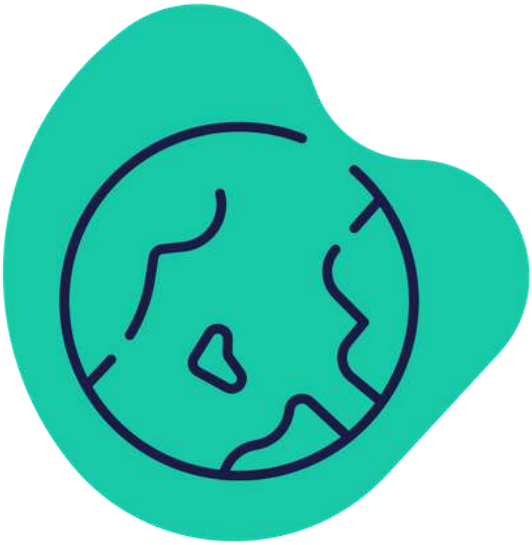
The UK has been subject to GDPR which has meant businesses have policies, processes and procedures in place to protect data and privacy inline with the regulation. Even though the UK has left the EU, there is now a UK version of the GDPR in domestic law. This together with the Data Protection Act 2018 forms the backbone of the UK's data protection regime.

Currently, at least, the UK GDPR and the EU GDPR are materially the same. However, over time it's inevitable that there will be some divergence on both sides. This will become particularly important if your organisation processes data in both the UK and EU, as you'll need to identify which version of the GDPR should apply to each set of data that you're processing.

International transfers

Whichever version of the GDPR you're working with, it's important to be aware of the restrictions in place concerning international transfers - particularly in today's wonderful world of cloud services and increased remote working.

The default position in the GDPR is that international transfers should only be made where the receiving country provides an adequate level of data protection. This basic principle is to ensure that data subjects enjoy equivalent rights (and also that these are enforceable) as they would in a country where the GDPR applies.



If the country you're transferring to is not considered adequate, then you'll need to put in place what the GDPR calls "appropriate safeguards".

The GDPR outlines several possible approaches to this, but the current guidance is clear, that it's not just a box-ticking exercise and the transferring party has a duty to ensure that whatever safeguards they put in place are effective.

Which countries are adequate? Well, so far, a relatively small number of countries have made the cut, and some of the names not on the list may surprise you - for example, the United States is currently not considered to be adequate for the purposes of the GDPR. This of course can have important implications when working with 3rd parties.

Working with 3rd parties (including transcription providers)

It's not uncommon for researchers to use third parties for a variety of purposes.

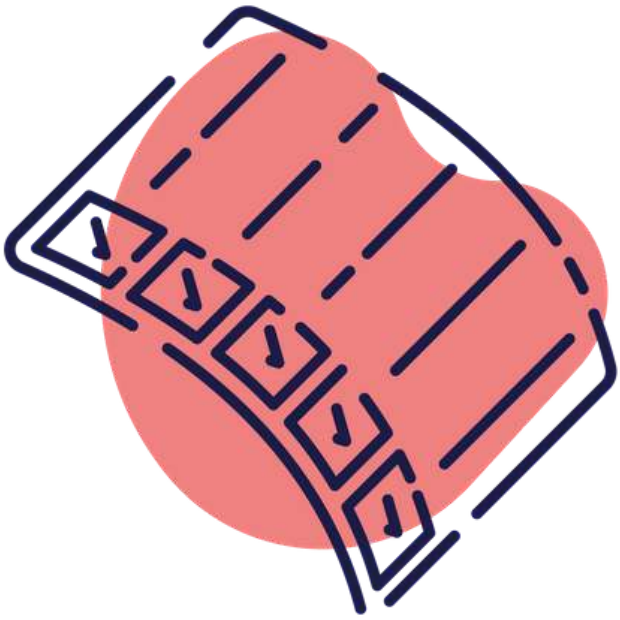
This includes third party software such as text analytics, Automatic Speech Recognition (ASR) and survey platforms. As well as utilising other services such as human-based transcription - that's us!

If you're at an agency, you're the one who has the contract with the client, or if you work at a brand, it's you the participants have put their trust in.

So, either way, it would be devastating if all your hard work to make sure your practices are secure, falls down at this stage.

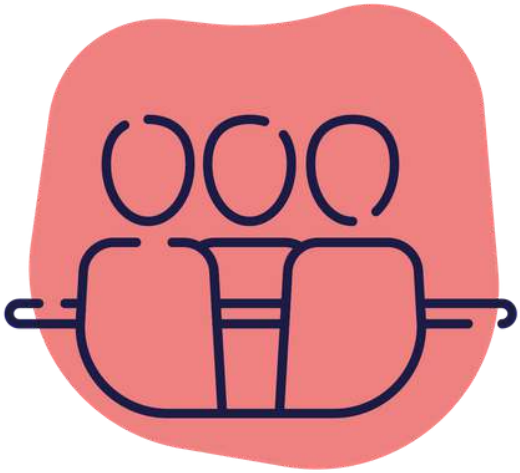
This isn't to say third parties suppliers aren't secure, they certainly can be, but it's your responsibility to do your due diligence on the suppliers you select. It's also good to remember that for GDPR compliance, any processing done on behalf of the data controller must be governed by a written contract.

Here are some of the important aspects to consider, some you may already be aware of, but others may give you a new perspective.

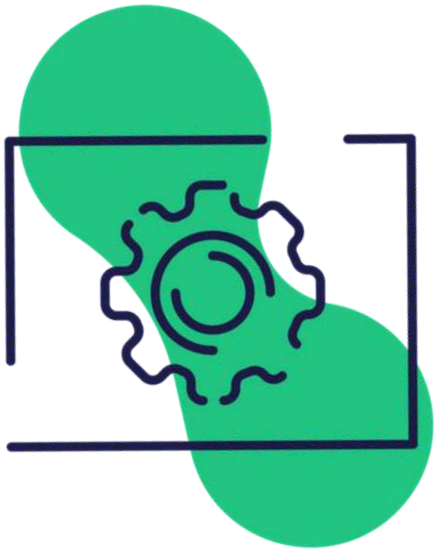


Who has access to your information?

Is data locked down as much as possible or do many, potentially 1000's of people, have the ability to access any information and content you provide? As we mentioned, human error is a big problem, so minimising access is usually a good idea.



Where are the people based who have access to your information? It can be challenging to pursue any security violations should they occur when any workers are based in a different location, even if a Non-Disclosure Agreement (NDA) is in place.



In the case of Take Note we provide secure portals for you to upload content to, we also only provide access to the content to those directly involved in the project (typically the transcriber & account manager). Transcribers carry out the transcription within a secure environment, they can't download the files to their computers. Once your transcript is completed and quality checked, you retrieve it via a secure portal.

HTTPS websites & portals where you are sharing information

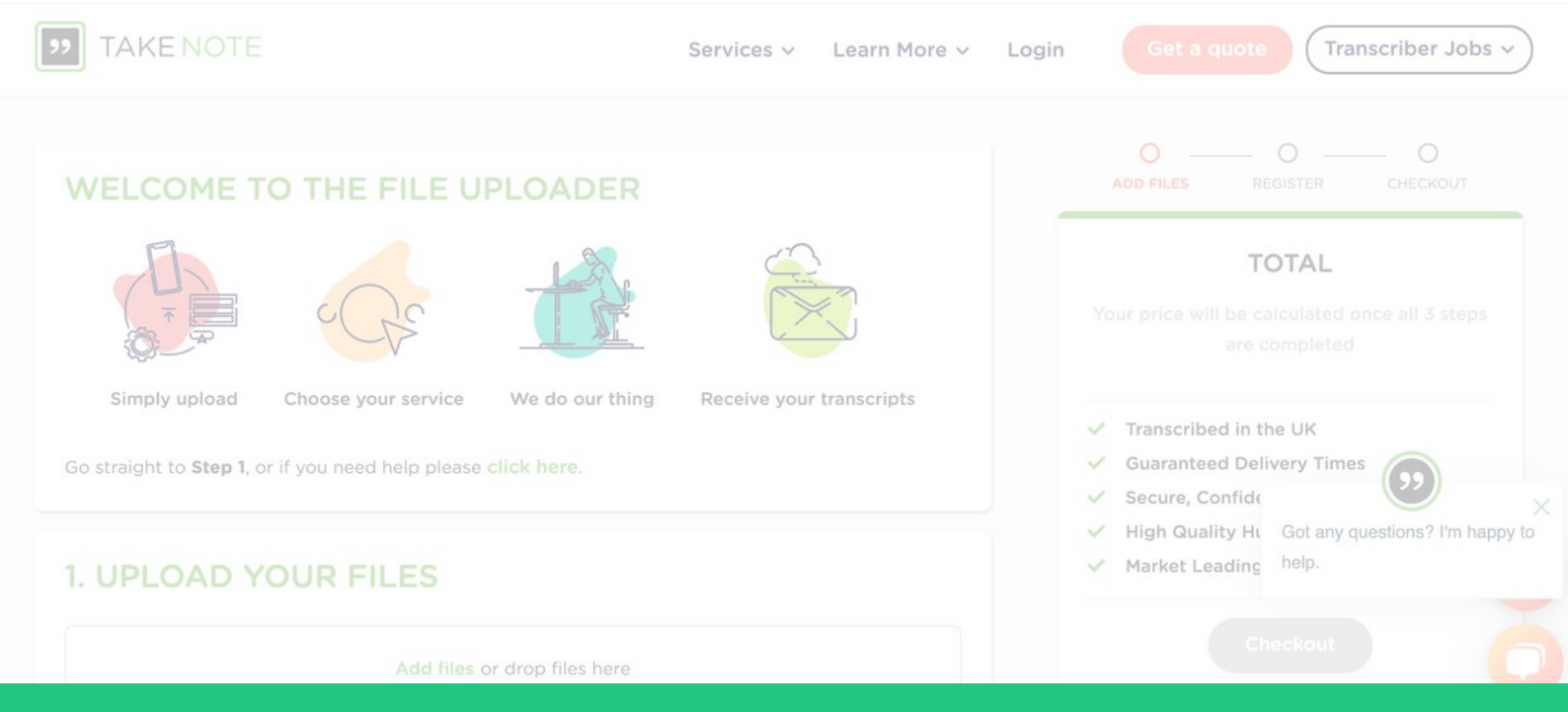
HTTPS is a secure version of the transfer protocol which is used to send data between a web browser and a website. This basically means that data transfers are more secure as the data is encrypted. On an HTTP site, the data transfer isn't encrypted, and so any intercepted data can be easily read.

Whenever you enter any details into a site, be sure to check that the site is HTTPS rather than just HTTP. This is good practice to follow, not just for work purposes but for any personal browsing too.

There are a few ways you can check for this:

- View the full URL and check that it starts with 'https://'
- Look for the padlock in the browser address bar
- Ensure you do not see any 'this website is not secure' messages

Think of this as the first line of defence. However, there are additional signals of a secure service that you should also look for.



What processes are in place?

We've talked about the importance of processes and procedures to minimise risk and the same applies to third parties that you're sharing data with:

Are any servers locked down as much as possible to restrict access?

Security-conscious companies will require authentication to access data and may also limit access to specific IP addresses.

Can your content be downloaded to a non-secure environment or copies be made to external storage?

Ideally, your data should be held within secure, encrypted environments at all times.

Is the third party relying on Data chunking?

This process splits your data into chunks so if there were to be a breach, they would only have a small piece of the puzzle.

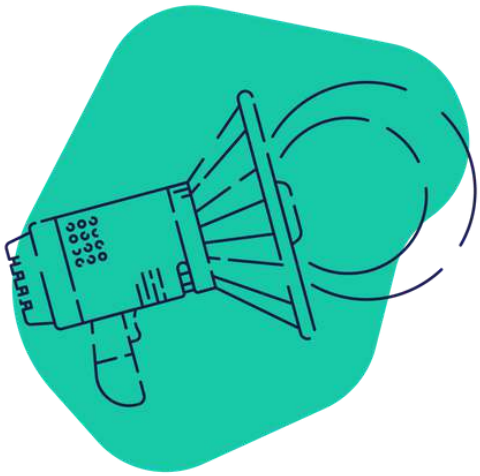
Although it makes it challenging, it's not a guarantee. There is still a risk if other, more stringent measures are not in place.

What indications are there that a supplier takes data security seriously?

They shout about it

Well, they don't have to literally shout, but they may raise their voice slightly or use a bold font! If companies have invested in security they will have this information readily available for you, usually on their website. If you can't find what you're looking for, get in touch, as it should be easy for them to provide you with their security credentials.

They may even have their very own Owen (they won't be as good as ours, but they get points for trying).



ISO certifications

If you've ever been through an ISO certification, you'll know they are pretty extensive and intensive! Companies will have dedicated resources to not only achieving their certifications but in their ongoing management of the associated processes and systems too. It provides a rubber stamp from an impartial third party that they meet the required standards.

The certifications to look out for are ISO 27001 and 9001. ISO 27001 relates to all aspects needed for a robust information security management system (ISMS).

It's also worth checking what aspects of a business the ISO certification covers. It's not uncommon to find that an organisation has an ISO 27001 certification covering only a limited scope of their ISMS, their data centre, for example, which may leave large gaps in how they manage information security more generally.

ISO 9001 sets out the criteria for a quality management system with a strong customer focus.

ISO 27001 is internationally recognised and is often seen as the gold standard for ISMS, covering all forms of information, including digital.

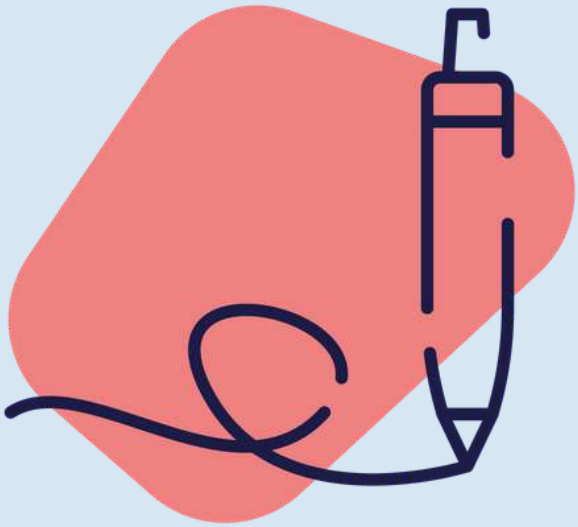
You may also come across Cyber Essentials and Cyber Essentials Plus. These certifications are part of an assurance scheme backed by the UK Government which is designed to help organisations get to grips with the basics of cyber security and guard against common cybersecurity threats.

Willingness to sign Non-Disclosure Agreements (NDAs)

Even when a company has put in a vast array of security measures to minimise risk, it's impossible to eliminate it altogether.

You might find that your company requires that any third parties sign an NDA, to assign greater legal accountability for any data. This can provide you with an additional layer of reassurance and also can act as a warning sign if a company refuses.

Remember though, when individuals are based in different countries it can be difficult to effectively pursue violations, so don't rely on an NDA only.



Helpful Resources

We've aimed to touch on the core elements of data security and compliance that you're likely to need to be aware of in the Market Research field. Here are some additional resources you might find useful that explore these topics in more detail.

ICO - https://ico.org.uk/for-organisations/dp-at-the-end-of-the-transition-period/data-protection-now-the-transition-period-has-ended/the-gdpr/
ISO - https://www.iso.org/home.html
MRS - https://www.mrs.org.uk/
ESOMAR - https://www.esomar.org/what-we-do/code-guidelines/esomar-data-protection-checklist
https://www.esomar.org/uploads/public/knowledge-and-standards/codes-and-guidelines/ESOMAR_Briefing-Questions-When-Considering-Tools-and-Services-for-Unstructured-Data.pdf

Sources

1 - CybSafe analysis from the UK Information Commissioner's Office (ICO)

You made it! Thanks again for choosing this guide.

We hope it's helped you to feel more confident about data security and compliance and provide you with some useful tips and best practice.

If you have any questions on data security, or about our transcription services, we'd love to hear from you.

You can get in touch with us:

info@takenote.co

https://takenote.co

+44 (0)207 928 1048

Stay safe out there!

TAKE NOTE