PEOPLE FOR RESEARCH

GDPR GUIDE FOR USER RESEARCH

Everything you need to know to ensure your research remains compliant.

ABOUT PEOPLE FOR RESEARCH

At People for Research we specialise in providing participant recruitment for user research and usability testing. We work in partnership with clients including global technology companies and government departments.

The driving force behind our service is a commitment to help the UX sector deliver valuable insights by providing reliable and high-quality recruitment of people for research. Our process enables clients to focus on what they do best while we identify, screen, and book reliable and relevant participants.

Over the last three decades, we refined our user recruitment techniques and turned them into part of our tried and tested process to find the best participants to take part in your projects, assuring the quality and validity of our data. Thanks to years of experience, we have developed a consultative approach and robust screening and booking process that translates into one of the industry's lowest drop-out rates.

Find out more about our services here or get in touch by emailing info@peopleforresearch.co.uk.

OUR SERVICES

- **Consumer recruitment:** connecting you with a diverse range of everyday consumers.
- **B2B recruitment:** sourcing senior professionals and business owners.
- **International recruitment:** accessing participants from around the globe.
- **Unmoderated recruitment:** providing participants for unmoderated surveys and tasks.
- **Panel management:** building and managing bespoke panels of participants.
- **Low digital recruitment:** engaging participants with limited digital access.
- **Accessibility recruitment:** recruiting individuals with disabilities to ensure accessible and inclusive research.
- **Accessibility Collective:** a dedicated panel of participants with access needs at a fixed price per head.
- **Customer data recruitment:** utilising your customer data to recruit participants for targeted research.
- **Incentive management:** managing your participants' incentives on your behalf.
- **Recruitment & studio:** providing a full suite of recruitment and studio services.

GDPR BASICS

If you already know the basics about the General Data Protection Regulation (GDPR), then feel free to skip this section.

The GDPR superseded the Data Protection Act from 1998 on 25th May 2018. Since then, GDPR has imposed more requirements on organisations to think about how they securely manage all personal data that they hold and how they process this data. Individuals have stronger rights to their privacy and if organisations can't show that they are taking measures to meet these rights, significant fines can be imposed.

What is the GDPR?
The General Data Protection Regulation is a regulation in EU law on data protection and privacy in the European Union and the European Economic Area. The GDPR is an important component of EU privacy law and of human rights law, in particular Article 8 of the Charter of Fundamental Rights of the European Union.

What is personal data?
Any information that relates to an identified or identifiable living individual.

Is all data the same?
No, all identifiable data that relates to a living individual is personal data, but some data is special.

What is special category data?
The current legislation singles out some types of personal data as likely to be more sensitive, and gives them extra protection. This includes:

- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- criminal record;
- data concerning a person's sex life;
- person's sexual orientation;
- genetic data;
- biometric data (used for identification);
- and/or health data.

To have a compliant privacy policy that also covers your user research needs, you will need to define the following:

The **type of information** you will collect from your different audiences, website visitors, customers, etc.

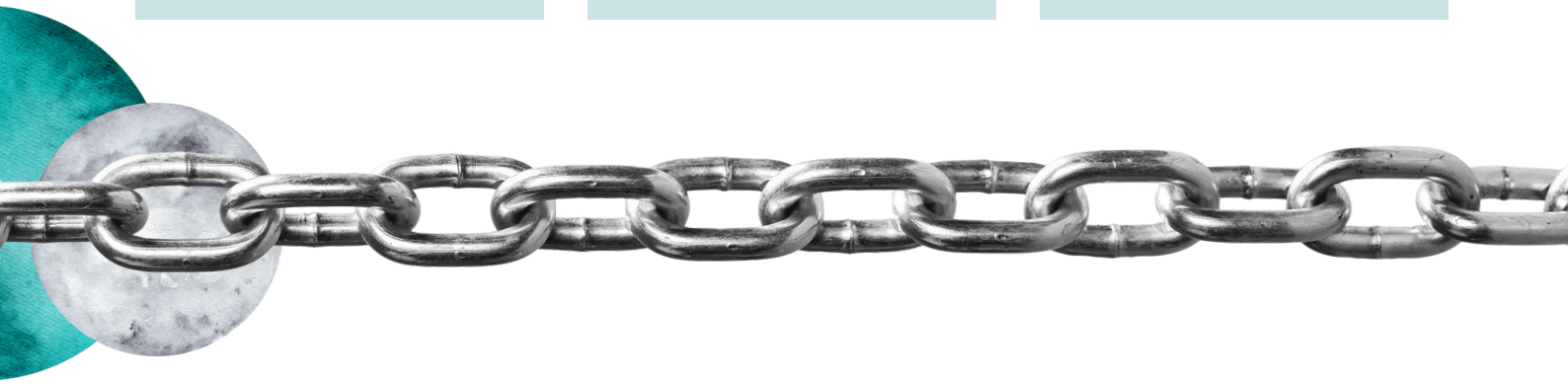
The reasons for **collecting** the personal data and how you do this.

How your organisation is **planning to store** the individuals' personal information.

The **lawful basis** your organisation is relying on for processing personal data (e.g. informed consent).

The individuals' **data protection rights**, including timeframes for deletion of their personal data.

How individuals can **contact your organisation** to complain, request the erasure of their data, request a DSAR, etc.



You will also need to be aware of GDPR roles, especially if you are partnering with an external recruiter or you work for an agency collaborating with an end client.

Controller of data
The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Controllers make decisions about processing activities. Within the definition of Controller, you can also have sub-roles such as Independent Controller or joint Controller.

Processor of data
The natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller. Processors act on behalf of the relevant Controller and under their authority.

Sub-processor of data
A third-party processor engaged by a Processor who has or will have access to or process personal data from a Controller. In order to use a Sub-Processor, the Processor needs to have the Controllers' written permission.

GDPR CHECKLIST FOR USER RESEARCH

- ☑ Be clear at the point of collection of data why you need the individual's information and let them know.
- ☑ Be clear about the length of time you are going to hold personal data and let the individuals know.
- ☑ Make sure you have a privacy policy that includes all the relevant information in clear and concise language.
- ☑ Make it clear to individuals what you plan to do with their data when you collect it. Give individuals a clear and easy option to refuse marketing activities and communications.
- ☑ Be accountable and understand your responsibility to be compliant and be prepared to demonstrate this by regularly recording your activities, always taking into account your organisation's legal grounds for processing personal data across different scenarios.
- ☑ If asking for informed consent, don't assume it is given by default – always ask individuals to positively opt in.
- ☑ Give individuals options to consent based on what the different ways the data will be used.
- ☑ Keep records of when and how you got consent from individuals.
- ☑ Name your organisation and the individual in the organisation responsible for data protection in any relevant documentation and, if applicable, the type of third-party organisations you are proposing to share data with.
- ☑ If applicable, tell individuals that they can withdraw consent and show them how to do so, without detriment.
- ☑ Allow individuals the right to delete their accounts or personal information where they withdraw their consent to the processing of their data.
- ☑ Implement a level of security for the stored personal data appropriate to the risk by carrying out a privacy risk assessment. Regularly test, assess and evaluate the effectiveness of the security measures you put in place.
- ☑ Create protocols around any security breach to make sure you report these to the supervisory authority (the ICO) no later than 72 hours from when you become aware.

PROTECTING USER DATA AT ALL STAGES

Before research

1. Ensure the privacy policies and terms between all partners accessing the data are up to date and relevant. Policies should state what data is collected, intended purpose of use, how data is stored and for how long, and how to request the deletion of data.

2. Set rules around data sharing – for example, never use email to share participant data openly. If sharing data with your team or clients, make sure it's pseudonymised/anonymised.

3. It can be very handy to print/download a copy of your research documents if you aren't sure you can view them online. Print immediately before the session(s) and keep it on your person at all times.

During research

1. Keep all research notes captured during your sessions pseudonymised.

2. If recording a research session (video/audio), make sure you have the participant's informed consent and attempt to omit or edit out any personal data, unless it's critical to the research.

3. Try not to capture any real personal data, unless it's critical to the nature of the research. For example, if testing a form, allow the user to input dummy data.

4. When conducting high-volume online surveys or tasks, collect as little user data as possible by providing users with a unique ID that they can use as their identifier and avoid capturing IP, geolocation or audience analytics.

After research

1. If any research documents have been printed or downloaded, ensure these are physically destroyed or permanently deleted. Any documents that need to be kept post-research (e.g. signed consent forms), must be stored in a secure manner.

2. Store all video/audio files on a secure location or machine. If using a cloud-based service, ensure their policy meets GDPR guidelines. You should also limit who has access to the files.

3. On completion of a project, all shared documents should have access permissions revoked, preventing ongoing access to user data (e.g. participant screeners, time plans, etc.)

4. Ensure that data deletion or destruction protocols are being followed.

CREATING A COMPLIANT CONSENT FORM

Consent forms are intended to outline the terms and conditions regarding participation in something or acknowledge the release of an individual's information. Without a consent form, it's considered unethical and in some cases illegal to allow a person to participate in an event or study or for the release of their information.

Your consent form must include information about the following:

- Who is keeping and accessing the data.
- How the data will be handled and what it will be used for.
- The lawful basis for participation in the study (e.g. informed consent).
- Make it clear if you are recording video or audio during the session.
- What is required from the participant so their participation can be considered successful and what they need to do to receive their incentive, if offering one.
- A link to your organisation's privacy policy.
- An email address (or other form of contact) that the participant can use to request the permanent deletion of their personal data.

Building a compliant and straightforward consent form.

- On a regular consent form, where the participant is allowed to know the identity of the organisation running the research, it is ideal to have the organisation's logo on the document.
- Start by defining the identity of the parties.
- Provide a summary of the research study or task.
- If offering an incentive, confirm the sum that will be offered upon completion of the study.
- Collect the following information so the participant can be identified and the consent form can be validated:
  - first and last name
  - email address
  - signature
  - date of signature

TOP TIP

Try to keep the consent form as short (ideally, it will be a one-page document) and simple as possible and make sure you use language that is easy to understand. It's essential to avoid industry jargon, as well as going down a heavy legal route, which could make the document "scary" for your participants and might even cause them to drop out from your research.

If you feel, however, there is non-compliance-related information that should be included in the document (e.g. logistic information about a study), save this as an online document or a webpage and add it as a link to your digital consent form.

Visit the Resources area on our website to download our consent form template.

USING AN EXTERNAL USER RECRUITER?

People for Research conduct all our user recruitment in-house, therefore we can easily reassure clients that we have the appropriate processes in place.

If you are not working with PFR, here are some top tips to help you determine if your user recruitment supplier is compliant or not.

1. Ask your recruiter who is screening participants, if they are compliant, and how they are managing the data exchange between all parties involved.

2. Check what data they will be capturing during the screening process and what will be shared with you.

3. Ask how they store participant data and find out more about their GDPR policies.

4. Check how they intend to share data with you and whether this is in line with your own GDPR policy.

5. Confirm if they are able to distribute your consent form on your behalf or not.

AGENCY WORKING WITH AN 'END CLIENT'?

Many of our clients are agencies who work closely with their clients, conducting user research on their behalf, and have stakeholders come along to view their sessions. This process involves revealing some information about the participants ahead of or during the research session.

Some top tips:

1. Define the GDPR roles between the parties and ensure your client is aware of your data protection policy.

2. Pseudonymise any personal data shared with the end client by removing identifiable details such as names or email addresses from any shared documents.

3. Use a tool such as SharePoint or Google Drive that limits access to shared documents. This reinforces the idea of responsibility and traceability.

4. If possible, set expiry dates on shared documents (this is something SharePoint allows you to do).

5. Inform participants how their personal data will be used during and after the research session. Do this before the session takes place, ideally by getting them to sign a consent form.

6. Be transparent, clear and use straightforward language that is easy to understand.

INVOLVING YOUR CUSTOMERS IN RESEARCH

The following tips should be treated as a starting point to recruit your own customers for user research or usability testing in a compliant manner.

Be transparent
It is essential to clearly explain how you will be using your customer's data if they are opting in to participate in research, and if you intend on passing their data to a third-party for processing.

Ask your customers to opt-in
Our recommendation based on the GDPR guidelines is to contact your customers with clear and specific details of what you want people to participate in, how they can be involved and, if working with an external recruiter, explaining their involvement to your customers. This is the ethical and responsible way of involving your customers in research or testing.

Manage opt-outs properly
Any communication that goes out to your customers should have an opt-out option; people have the right to withdraw consent at any point in the process.

Use a secure data transfer service
Use a secure data transfer service that encrypts information when sending data back and forth for review. We also recommend pseudonymising personal data, and removing anything that is not explicitly required for the purposes of running the research session. This minimises your risks of a data breach.

A GDPR must-have: informed consent
Make sure you give your customers the opportunity to participate based on their informed consent: this means they are happy with the terms of their involvement and what you will do with any information they share as part of a research or testing session. This should be done as part of the recruitment process.

Non-disclosure agreement?

Although this doesn't relate directly to data protection, it is a more general document that could be required in research and testing, it is easy to become complacent especially if you are just running a simple benchmarking study. However, the non-disclosure document (NDA) is not just for your benefit. It also confirms the intent of the research, and tells participants what they can and can't disclose to other people outside of the research.

THE LEADING USER RECRUITMENT AGENCY

We are recognised leaders in the field of participant recruitment. At People for Research, we specialise in providing participant recruitment for user research and usability testing. We work in partnership with clients including global brands, innovative start-ups and government departments.

Discover our GDPR compliance and quality-checking process.

Dedicated data protection specialist
PFR have an in-house dedicated data protection specialist who is responsible for all our policies and GDPR compliance.

ICO registration
We are registered with the Information Commissioner's Office (ICO) as data controllers.

Successful GDPR audits
PFR have successfully passed GDPR audits with Visa, Monzo, NatWest, BBC, and many other large organisations to be appointed on their agency roster.

Robust privacy policies
We have robust privacy policies in place, designed to specifically cater to and protect the rights of the different groups of people we work with.

Consultation and advice
Our data protection specialist is available to consult with clients and provide advice on compliance in user research or answer questions about our terms.

Get in touch!

As part of our services, we offer compliance advice. We believe in sharing our data protection knowledge and experience to ensure your research remains fully compliant.

info@peopleforresearch.co.uk

+44 117 921 0008

Contact us via our website

Empower your research insights.
Contact us today.