GDPR compliance: Brand Legacy Code of Conduct

V1: 18th May 2018 & reviewed & updated 1st February 2021

Overview of relevant business activities :

1. The principles of our response to GDPR
2. Recruitment, consent & collecting participant information
3. Disposal of personal information & handling of outputs
4. Protecting stored data & other outputs
5. Sharing information & outputs with suppliers
6. Sharing information & outputs with clients
7. Handling client data

1. Outlining the principles of our response to GDPR

Brand Legacy acknowledges the importance of paying due care and attention to the rules of the UK General Data regulation (previously Data Protection Act – Regulation (EU) 2016/ 679 of the European Parliament and of the Council of 27 April 2016) on the protection of natural persons with regard to the processing of personal data and on the free movement of such data – known as "GDPR"

The GDPR potentially impacts our business when conducting Qualitative research amongst the general population and it is in this capacity that we set out our Code of Conduct.

For our client contacts, we do not carry out any direct marketing, or hold any databases for the purposes of marketing / cold calling/ new business so we have not set out any guidelines in relation to these activities. We do of course periodically contact existing clients but this is on an individual basis.

As advised in GDPR guidelines we apply a balancing test to the handling of personal data of market research participants, ensuring we weigh both importance of the **fundamental rights and freedoms of the data subject*** with the **legitimate interests** pursued by the controller or by a third party, and Brand Legacy's "freedom to conduct a business". (Article 16 of the European Charter of Fundamental Rights).

*(*The data subject being an identifiable person who can be identified directly or indirectly by reference to an identifier such as a name, number, location or other profiling factors.)*

Our guiding principles are that we will always apply the following tests:

- The data subject has been made fully aware of how their details will be used and how any information they share with us will be handled
- All data subjects have given active consent to share their information and participate in projects with the full knowledge of above
- We will not use data for any purpose that was not set out with data subjects from the outset, or recontact them to request alternative uses of their personal data or outputs
- We will ensure that all suppliers and clients who may also have access to personal data or outputs have agreed to treat materials in the same way

2. **Recruitment, consent & handling of respondent information**

- At recruitment, all participants will be given a full and reasonable explanation of what they are being asked to do and will only be recruited if they give consent to this
- Participants are typically paid a financial gift when taking part in research. Our commitments to maintaining their privacy and their consent will be reconfirmed when they attend research and acknowledge receipt of this gift via a signature sheet with a statement relating to consent and alerting them to data capture techniques (example attached in Appendix)
- If audio/ video recording or photographic material is to be gathered, this will be made clear to participants, and we will gain their consent for it to be used for the explicit purposes set out to them, before engaging them in the project
- We will collect only the information necessary to the successful running of that project. This will include personal contact information but will also include profiling information as pertinent to the topic under consideration.
- We will ask recruitment suppliers to confirm that their activities are also compliant with the GDPR requirements.

3. Disposal of personal information & handling of outputs

- Personal contact information (i.e. full names, addresses, phone numbers) will be deleted 6 months after completion of the project.
- When quotes, images or video is included in output material such as debriefs, presentations and reports it will not be shared in association with a real name.
- We will sometimes show faces in the context of our output material but the participant will always be made aware when such photographic/ video material is captured that it will form part of the data set and could be shared with clients - but not in association with their real name or contact details. We will obtain their permission for this possible sharing.
- It is not practical within the successful application of our business activities to later retrieve and delete specific respondent information that has been gathered and shared in this way, so we will not offer to delete specific material shared by any respondent. However we will make every effort to ensure they cannot be personally located by anything we share with clients about participants profiles, views, habits & behaviours.

4. Protecting stored data & other outputs

- Electronic storage: Personal profile information will be stored in password protected files. Devices with access to such material will also be password protected.
- Paper storage: we will only print when absolutely necessary from a practical point of view (e.g. as checklists at group discussions, for maps and directions etc). Any printed information will be stored in project files belonging to the project manager team and every effort made to ensure they are kept securely. All paper records of names, addresses and phone numbers will be destroyed once the project is complete.
- We retain electronic copies of all our reports and outputs such as edited films and we ensure that this storage is password-protected on both devices and on the cloud.

5. Sharing information & outputs with suppliers

- All suppliers (e.g. freelance moderators, partner agencies, notetakers, interns etc.) will be asked to agree that they comply with our policy by signing a copy of this document and agreeing to abide by the practices and guidelines set out .
- All suppliers must agree to destroy any information they have been given by or about participants in association with their work with Brand Legacy

6. Sharing information & outputs with clients

- If our clients request access to source materials such as video /photographic / interview notes (i.e. original data collected rather than debriefs, presentations and reports) we will always make clear the terms on which these can be shared and obtain explicit agreement that its use will comply with our policy
- Clients must agree that the material will only be used for the purposes set out when participants' permission was given, as per the rules of the MRS.
- Unless explicitly stated to participants this will mean that it can be used only within the business as a source of insight and information only. It will not be shared directly with their own clients, retailers or suppliers unless explicit permission was given at the outset of the project by participants. We will not go back to data subjects to request such permission retrospectively as this would contravene our code of conduct.
- When sharing this information Brand Legacy will not link any outputs to participants' names, addresses or phone numbers, or any other explicit identifiers which could facilitate the tracing of the data subject.
- Clients must also agree to comply with all other aspects of our Code of Conduct in handling this material (i.e. not link it to names / addresses / numbers / other identifiable profiling data if sharing internally).

8. Handling client data

- Brand Legacy is occasionally asked to use client databases to recruit and contact participants in our research projects. In this situation we will:
- Use the data only in accordance of the agreement with the client on providing such data
- Not modify, alter or amend the contents
- Not share the data with another sub-contracted organisation unless explicitly agreed with the client and in pursuit of the application of the project agreement (e.g. sharing with recruitment suppliers)
- At all time take precautionary measures to protect the data (e.g. password protections)
- Ensure access is only given to the necessary members of the direct team and that they are aware and consent to treat the data in the ways set out in this Code of Conduct
- Make the client immediately aware of any requests from data subjects to have access to their data or to remove them from the database.
- Make the client aware of any complaints in relation to the handling of their data
- Make the client aware immediately of any loss of data or breach of privacy in relation to the data set provided to us
- On completion of the project, we will destroy and/or return documents containing or incorporating the client's data and obtain confirmation that any sub-contactors have done the same.