Data Protection Policy

Updated: April 2018

Data Protection Policy

1. Introduction

Revitalise needs to collect and use certain types of information about the guests, volunteers and staff who come into contact with us in order to carry on our work. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material and there are safeguards to ensure this under the General Data Protection Regulation (GDPR) (EU) 2016/679 and the Data Protection Bill 2017.

2. Data Controller

Revitalise is the Data Controller under the Regulation, and John Parker is the Data Protection Officer, which means that he determines what purposes personal information held, will be used for. He is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

3. Disclosure

Revitalise may share data with other agencies such as the local authorities, funding bodies and other voluntary agencies, if there is a lawful reason for the sharing.

The guests, volunteers and staff will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows Revitalise to disclose data (including special categories of data) without the data subject's consent.

These are:

a) Carrying out a legal duty or as authorised by the Secretary of State

b) Protecting vital interests of a guest, volunteer, staff person or other person

c) The guest, volunteer or member of staff has already made the information public

d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights

e) Monitoring for equal opportunities purposes – i.e. race, disability or religion

f) Providing a confidential service where the guest, volunteer, or member of staff's consent cannot be obtained or where it is

reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill guests or volunteers to provide consent signatures.

Revitalise regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal.

Revitalise intends to ensure that personal information is treated lawfully and correctly.

To this end, Revitalise will adhere to the Principles of Data Protection, as detailed in the General Data Protection Regulation 2016.

Specifically, the Principles require that personal information shall be:

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject;
2. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes;
3. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or in accordance with Article 89(1) subject to implementation of the appropriate technical and organizational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject
6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures.

And that Revitalise as the Controller shall be responsible for, and able to demonstrate compliance with all of the above.

Revitalise will, through appropriate management and strict application of criteria and controls**:**

- Observe fully conditions regarding the fair collection and use of information

- Meet its legal obligations to specify the purposes for which information is used

- Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements

- Ensure the quality of information used

- Ensure that the rights of people about whom information is held, can be fully exercised under the Regulation. These include:

    - The right to be fully informed of how their data is being processed,

    - The right of access to one's personal information

    - The right to prevent processing in certain circumstances

    - The right to correct, rectify, block or erase information which is regarded as wrong information)

    - The right to be forgotten

    - The right of portability of data to another organisation

- Take appropriate technical and organisational security measures to safeguard personal information

- Ensure that personal information is not transferred abroad without suitable safeguards

- Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information

- Set out clear procedures for responding to requests for information

4. Data collection

Informed consent is when

- A guest, volunteer or member of staff clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data

- And then freely gives their consent.

Legitimate interest is when

- Revitalise has collected data prior to the General Data Protection Regulation coming into effect, or has collected it without the necessary consent for its use.

- Revitalise needs to use the data to fulfill its operational needs or to comply with legal requirements, for example for commercial interest, or for broader societal benefit.

- Revitalise reasonably expects that using the data would have a minimal privacy impact, or there is a compelling justification for the processing.

- Revitalise has balanced its own needs against the individual's interests, rights and freedoms, and reasonably believes that the processing would be expected by the individual, and would not cause unjustified harm.

Revitalise will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, by telephone, or by completing a form.

When collecting data, Revitalise will ensure that the guest, volunteer or member of staff:

a) Clearly understands why the information is needed

b) Understands what it will be used for and what the consequences are should the guest or volunteer decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed

d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress

e) Has received sufficient information on why their data is needed and how it will be used, including all the types of processing that may take place

5. Data Storage

Information and records relating to guests, volunteers and staff will be stored securely and will only be accessible to authorised staff and volunteers.

Revitalise will create and maintain:

- a personal data map, which lists all of the places in which it holds data, where it comes from and who it is shared with.

- a data processing register, recording all the occasions data was processed.
- A record of consent, covering the consent wording used, how and when the consent was acquired, and whether it has been withdrawn subsequently

Information will be stored for only as long as it is needed, or as long as consent has been secured for (whichever is the shorter), or as required by statute, and will be disposed of appropriately. The types of information we hold and the length of time we will store them are listed below, unless you request otherwise.

Information	How long we keep it	Why we keep it
Information about our guests	8 years from last contact	To let you know about our latest brochures and news, and to investigate complaints
Information relating to an enquiry you have made	8 years from last contact	To let you know about our latest brochures, news and offers
Details of visitors to our centres	8 years from last contact	To let you know about our latest brochures, news and offers
Information you give us on our website	8 years from last contact	To give you information you ask for, and let you know about our latest brochures, news and offers
Information about our supporters	8 years from last contact	To say thank you, share our latest news, and let you know about ways you can help
Telephone calls we have recorded	2 years	For training and monitoring, and to investigate complaints
Volunteer registration information	8 years from last contact	For financial auditing, and to investigate complaints
Volunteer bank details	6 years	To pay your expenses, and then subsequently for financial auditing
Volunteer enquiries	5 years	To keep you informed of volunteering opportunities, unless you opt out

It is Revitalise's responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation, which has been passed on/sold to a third party.

It is Revitalise's responsibility to ensure that all personal and company data passed to an external third party, such as a mailing house or a research survey company, is shared securely pursuant to the terms of GDPR compliant data processing agreement and destroyed after use.

6. Data access and accuracy

All guests, volunteers and staff have the right to access the information Revitalise holds about them. Revitalise will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.

In addition**,** Revitalise will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection

- Everyone processing personal information understands that they are contractually responsible for following good data protection practice

- Everyone processing personal information is appropriately trained to do so

- Everyone processing personal information is appropriately supervised

- Anybody wanting to make enquiries about handling personal information knows what to do

- It deals promptly and courteously with any enquiries about handling personal information

- It describes clearly how it handles personal information

- It will regularly review and audit the ways it holds, manages and uses personal information

- It regularly assesses and evaluates its methods and performance in relation to handling personal information

- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

7. Practical steps

Paper data storage

- When data is stored in paper form, it must be kept in a secure place where unauthorised people cannot see it

- When not required, paper files containing data shall be kept in a locked drawer or filing cabinet.

- Staff must ensure that paper and printouts are not left where unauthorised people can see them, like on a printer, or a desk overnight

- Data printouts must be placed in the secure disposal bins or shredded, when no longer required.

Electronic data storage

- Data must be protected by strong passwords that are changed regularly and never shared with anyone.
- If data is stored on removable media, like a USB stick or CD, the data must be encrypted and these must be locked away securely when not being used.
- Data must only ever be stored on TS-Farm, and not on local drives or servers.
- Data must never be saved directly to laptops or other mobile devices, like tablets or smart phones.

Data use

- When working with personal data, staff must ensure that the screens of their computers are always locked or turned off when left unattended during the working day.
- All computers must be properly closed down at the end of the working day.
- Personal data must never be sent by email, either in the body of the email or as an attachment, as this is not secure.The encryption tool must be used.
- Data must be encrypted before being transferred electronically.
- Personal data must never be transferred outside of the European Economic Area.
- Staff must never save copies of personal data to their own computers. Always access and update the central copies of data within TS-Farm.
- Data must be held in as few places as possible. Do not create unnecessary additional data sets.
- Staff must take every opportunity to ensure data is updated. For example, by confirming a guest's details when they call.