General Data Protection Regulation

Updated 11-07-18

Notice to reader - This is a working document that will continue to evolve as needed to address the General Data Protection Regulation and its relevance to the use of software and services by Better Impact. It is a statement of the undertaking by Better Impact to ensure that in its role as a data processor, it is compliant with the GDPR. Although suggestions for implementing the GDPR in our software are included, this is for your convenience only and should not be considered legal advice for your organisation.

Important Note
More than once in the regulations you will find the wording "Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons…". With this it is apparent that it was the conscientious intent of the regulation authors to address a very wide range of data collection realities. Our approach embraces this intent and seeks to be an applicable balance between all factors listed by the regulation authors in the line quoted above.

This document is intended to provide a comprehensive understanding of the use of Better Impact software related to the GDPR. If you require a custom questionnaire completed, we are happy to undertake the work but as a custom service unique to your organisation, a fee of £75/hour and one hour minimum applies.

Article 6 – Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
f) processing is necessary for the purposes of the legitimate interests pursued by the controller[1] or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

[1]It is our opinion that paragraph (f) covers the processing of data related to all of your volunteers (except youth) and to the degree that historical data is needed for the operation of your organisation, past volunteers as well.

If you would like to additionally address the principle of lawfulness of processing further based on (a), please refer to Article 7.

Article 7 – Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

In Volunteer Impact – In the message you add to the Volunteer Policies text box associated with each application (Under Configuration >> Organisation Settings >> Application Form setting) insert your wording to indicate volunteers are giving consent for data processing in Volunteer Policies box and tick the box requiring volunteers to accept this. The date of their application serves as the date of their acceptance as there is no way to access and complete the application form without affirmatively agreeing to the statements presented. In Version 4.26 the wording of the title and acknowledgement button will become customisable.

To report on the date the gave their consent, you can run a personal profile export showing the date the volunteer joined your organisation. A saved copy of the acknowledgement wording saved in the Document Library can be used to demonstrate the wording used to which the volunteer gave consent.

If you still have volunteers complete a paper application form, you will need to include the same messaging and the opportunity for the volunteer to indicate their acceptance. You could then scan the document and store it in a Custom Field in their profile.

Additional Recommendations

- In the Application Form Settings section, tick the box to display this messaging right in the page (rather than requiring that volunteers click a link to open a panel displaying the messaging.)
- Add a PDF of this messaging, including the date that it or any amendments to it became affective, to the Document Library. Include the date that it became affective in the title for easy reference.

3. The data subject shall have the right to withdraw his or her consent at any time.[2]

In Volunteer Impact – A volunteer can Archive themselves through MyVolunteerPage.com (and you can Archive a volunteer through the administrative interface~~).~~ An Administrator can set their notifications so that they will receive an email alert if a volunteer Archives themselves. This is under Main >> Edit My Profile >> Miscellaneous Tab under Admin Settings – check off 'Volunteer Status Change Notifications'.

[2]This should not prevent you from being able to store information about a volunteer if processing is being made lawful by means describe in article 6, Paragraph 1 (b) or (f). Once these no longer apply however, the withdrawal of consent must trigger an end to the data processing.

Article 8 - Conditions applicable to child's consent

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

In Volunteer Impact – Although "the offer of information society services" does not seem to include the notion of processing data related to engaging a youth as a volunteer, there is a mechanism by which the consent can be authorised by the holder of parental responsibility. Include a pdf form for the youth to download in the document library and in the description of an applicable age related Custom Field or Qualification. Provide instructions to have the form filled in by the responsible adult, take a photo with a smart phone and upload to a Custom Field added to your Volunteer Impact Account for this purpose.

Article 9 - Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:
(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

In Volunteer Impact – Health data provided by a volunteer under questions such as "Do you have any health concerns of which you would like us to be aware?", can be asked, if applicable to your circumstances of volunteer engagement, given that it takes an action on the volunteer's part to provide it.

Demographics for statistical analysis should be collected in a separate survey tool that does not include any fields that could be used to identify the data subject.

Article 13 - Information to be provided where personal data are collected from the data subject

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In Better Impact software – In the messaging visible to your constituents prior to them giving consent, you need to include the point that that the data will be processed outside of the EU. Specifically, we suggest including the following:

> Personal data will be processed in a manner compliant with the ICO and the GDPR. It will be stored in Canada, one of twelve countries outside the EU that the European Commission has determined favourable for data storage.

If the controller wishes to prevent Better Impact support staff in the USA or Australia to access data to provide for more user support options, it must choose to make this restriction within its administrative interface.

2. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

In Better Impact software – In the messaging visible to your constituents prior to them giving consent, you should inform them of your organisation's data retention policies and additionally what happens to the data after you remove them from your database.

In describing your policies, you might consider different retention rationale at different stages of a constituent's lifecycle with you. Some examples are listed below.

Volunteer Impact

1. Data required as part of the onboarding process but no longer required once a volunteer has been accepted, *will be deleted at that point in time and absent from any backups 28 days later.**
2. Data required while a volunteer is considered to be part of the pool of volunteers (active or inactive) but no longer required once a volunteer is no longer considered to be part of the pool of volunteers will be deleted semi-annually no greater than six months after that point in time * and absent from any backups 28 days later.
3. Data that is required as a matter of record after a volunteer is no longer considered to be part of the pool of volunteers will be deleted *annually no less than two years and no greater than three years** after that point in time and absent from any backups 28 days later.
4. Volunteers will be able to log in to have access to a record of hours contributed for a period of no less than one year and up to two years later. If a volunteer prefers that the record of hours contributed remain in place, logging into the volunteer portal will preserve the record for an additional period of no less than one year and up to two years after the login date.
5. Once an organisation removes a volunteer from the database, contact information (name, address, email address(es) telephone number(s)) and a record of volunteer hours contributed will remain in the Better Impact system for the volunteer's use until it is removed automatically no less than two years and no greater than three years after the profile was last accessed by the volunteer, or by request from the volunteer.

**Your organisation can specify the timing in orange italics.*

Additional Recommendations

- In the Application Form Settings section, tick the box to display this messaging right in the page (rather than requiring that volunteers click a link to open a panel displaying the messaging.)
- Add a PDF of this messaging to the Document Library

Article 17 - Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of a variety of grounds apply, including the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

Your organisation's application of Article 17 will, rightfully, vary based on the reason that data was collected and the rationale of what ought to be considered "no longer necessary".

In Volunteer Impact - If (**and only if**) a volunteer requests the right to be forgotten from the Better Impact system, you have the capacity to fulfill the request. Here are two examples of what you can do based on your application of Article 17.

1. If a record of hours, including the name of the person who performed those hours is all that is necessary to keep, replace all contact information except the name with random characters and then Remove (the term in Volunteer Impact) the volunteer. All that will be left of the data record you have access to will be the volunteer name and the hours log records. Additionally, Better Impact will have access to the IP addresses used to log in.
2. If a record of hours, along with some custom fields, volunteer trainings and other qualifications is required, simply delete the data in any fields where it is no longer required and archive the volunteer. This will reduce the data subject to the lowest level of data collection related to your needs.

Archiving vs Removing in Better Impact Systems

- Archiving – Committee association, General Interests, Signups, Assignments and placement on a Backup List will be deleted. All other data (Contact Details, Custom Fields, Qualifications, Notes, Communications History, Hours Log and Feedback Fields) remains accessible by your organisation. Volunteer contact information and hours logged remain accessible to the volunteer. Contact information remains editable by the volunteer. All data remains accessible to Better Impact. Your organisation remains the data controller.
- Removing – Only the volunteer's name and hours logged remain accessible by your organisation and neither are editable. Volunteer contact information and hours logged remain accessible to the volunteer. Contact information remains editable by the volunteer. Only Contact information, hour logs and IP addresses used to log in remain accessible to Better Impact. Your organisation is no longer the data controller.

Article 20 - Right to Data Portability

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and

(b) the processing is carried out by automated means.

2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

In Volunteer Impact – Given the degree to which Volunteer Impact is customisable, it is not technically feasible to have the data transmitted directly from one controller to another. It is, however, possible to provide the personal data to the volunteer in an Excel format.

Article 24 - Responsibility of the controller

1. *Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*

Our technical and organisational measures are a part of your technical and organisational measures. Please refer to Article 28 for some details on our measures.

Article 25 - Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

In Volunteer Impact

- Data minimsation – This is the area where you can most effectively apply the principles of data protection by design and by default. Review the Custom Fields, Qualifications and Feedback Fields configured in your account to ensure that you are only collecting the information absolutely required to properly engage volunteers, that you are collecting it only when you need it, and that you remove it when you no longer need it. For example:
  - If you do not onboard every volunteer who applies, consider what questions on your initial application form should be left to a later stage so that you are not collecting information that you don't yet need (e.g. emergency contact information, t-shirt size or food allergies etc.).
  - If you ask questions on an application that are used only as conversation starters in an interview, consider deleting that data at some point after the interview (e.g. most memorable volunteer experience, university attended etc.).

- Pseudonymisation – Pseudonymised data, is personal data that has been subjected to technological measures (like hashing or encryption) such that it no longer directly identifies an individual without the use of additional information. All data, with the exception of documents added to the Document Library or a rich text field (neither of which are designed to hold personal data) is encrypted at rest using 256 BIT AES encryption. In the event of a data breach on our server, all personal data would be unreadable.

- Anonymisation - Upon request by a volunteer, (and only by request*) you can anonymize the record by overwriting the contact information fields with non-identifying data. All other data in the record will remain intact.

*This is very important because you have no way of knowing if a constituent uses their profile with another organisation. The contact information is the only data to which this applies. All other data is related solely to your organisation.

Article 27 - Representatives of controllers or processors not established in the Union

Representatives of controllers or processors not established in the Union

Better Impact Software Ltd is a registered company in England and Wales. However, as Better Impact Inc. (of Canada) is involved in the processing as a subcontractor, Article 27 applies. The designated representative for Better Impact Software Ltd is Kate Saunders (kate@BetterImpact.co.uk, 020 3014 0226 Ext 152). In addition to our GDPR representative, any communications related to GDPR should also be copied to the CEO, Tony Goodrow (tony@betterimpact.co.uk, 020 3014 0226 Ext 120).

Article 28 – Processor

1. Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.

Highlights of our measures include:

- Data protection
    - All data, including backups are encrypted in motion and at rest
    - Firewalls tailored to permit the least possible amount of traffic
    - User session lock after a configurable period of inactivity
    - Two-factor authentication for Better Impact staff accessing data
    - Brute force protection
    - Automated intrusion detection with 24x7x365 human monitoring
    - Annual third-party penetration tests
    - ESET Antivirus software – updated as released
    - Complex passwords required by all administrators
- Our data centre
    - Facility monitored 24x7x365
    - Physical hardware is maintained behind locked server racks and cages
    - The system housing data records has no removable media access
    - CSAE4316, SOC 1 Compliant (Type 2 Report), (UTI) Tier III
    - Biometric authentication is required for access
    - Multiple fixed cameras covering all entrances and all cabinet rows with at least 90 days of retention
    - Access to the data centre halls required passage through a person trap
- Backups
    - Full back up once per week
    - Incremental backup once per day
    - Transaction log backup once every 3 hours
    - 28 days retention
- Resiliency

    - Guaranteed uptime (excluding planned maintenance) of 99.9% and a five-year history of 99.998%
- Application
    - Our SDLC process follows OWASP and the Microsoft Security Development Lifecycle
- Administration
    - Access to systems restricted to only uniquely identifiable accounts
    - Logged and auditable logins to the system
    - Annual staff review of data protection and confidentially policies
    - ISO 21001 certification expected in late 2018
    - Criminal background and reference checks on all Better Impact staff
    - ICO Registration # ZA051032

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Required Processors
Better Impact Inc. – Located in Canada
Cogeco | Peer1 – Located in Canada, the data centre where the Better Impact servers are located
ZeroFail - Located in Canada, service that stores our encrypted backups – They do not have the encryption key.

Please note: The Commission has given Canada a favorable determination of adequacy for data storage.

Optional Processors
Better Impact USA Inc. – Located in USA, processing related to providing support for client administrators
Better Impact Pty Ltd – Located in Australia, processing related to providing support for client administrators

Please note: The degree of user support we can offer outside of normal UK office hours is dependent on where data can be processed. Support can still be provided after hours but is limited to those questions that do not require accessing data to answer. By default, your account will be configured to prevent access to your data from Better Impact staff outside of the UK and Canada.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

Our new user agreement includes the following paragraphs:

1. The Processor will process the personal data only on documented instructions from the Controller, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. In agreeing to this licensing agreement, the Controller is providing written instruction to process any data it, or its prospective volunteer, current volunteers at any given time, or retiring

volunteers at any given time, add or edit in any of the Better Impact software the Controller utilises. In agreeing to this license, the Controller further agrees that the Processor may transfer the data to Canada. If the controller chooses to allow data transfer to the USA and/or Australia/New Zealand to provide for more user support options, instructions indicating so must be sent to GDPR_Regions@BetterImpact.co.uk.

2. The Processor will ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

3. The Processor will take all measures required pursuant to Article 32;

4. The Processor will respect the conditions referred to in paragraphs 2 and 4 for engaging another processor;

5. The Processor will take into account the nature of the processing, assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR;

6. The Processor will assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the Processor;

7. The Processor will, at the choice of the Controller, delete all the personal data after the end of the provision of services relating to processing, and delete existing copies unless Union or Member State law requires storage of the personal data and with the exception of contact information data related to volunteers who use or have used within the past five years, the same volunteer account with another organisation;

8. The Processor will make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

Article 30 - Records of processing activities

1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
b) the purposes of the processing;

We will be recording the purpose of the processing as the following:

- Regarding Volunteer Impact – To accept and record applications and/or expressions of interest to volunteer and maintain records related to the volunteer engagement and/or create volunteer rosters and/or track volunteer hours.
- Regarding Client Impact – To accept and record applications and/or expressions of interest to become a client and maintain records related to client assistance and/or client-volunteer interactions.
- Regarding Member Impact – To accept and record applications and/or expressions of interest to

become a Member and maintain records related to membership.

- Regarding Donor Impact – To accept and record donations along with the donor's contact information, and preference of donation allocation, and/or type of donation and/or associated campaign.

*2. Each **processor** and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:*
*the name and contact details of the processor or processors and of **each controller on behalf of which the processor is acting**, and, where applicable, of the controller's or the processor's representative, and the data protection officer;*
In Better Impact Software – Under configuration >> Organisation Settings >> Contact Information you will need to indicate your Data Privacy Contact and keep that information up to date.

Article 32 - Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

a) the pseudonymisation and encryption of personal data;

All data, with the exception of documents added to the Document Library or a rich text field (neither of which are designed to hold personal data) is encrypted at rest using 256 BIT AES encryption.

b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- confidentiality
  - data protection policies are documented
  - data protection policies are reviewed with all Better Impact staff annually
- integrity
  - imposed during the database design phase through the use of standard procedures and rules.
  - maintained through the use of various error-checking methods and validation procedures.
- availability
  - we guarantee that the servers will be up 99.9% of the time with the exception of planned updates
  - our five-year historical uptime is currently at or above 99.995%
- resilience
  - n+1 redundancy on everything except the database server (which is equipped with n+1 redundancy on the data storage drives)
  - support is offered from two separate locations in the UK and three other locations globally

c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

- All data is backed up to one server on site (for rapid restoration from a database hardware or data integrity issue) as well as to two separate offsite locations (for larger data centre issues).
- Our data centre has multiple locations into which we could re-establish the servers in a worst-case scenario.

d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

- Third party penetration tests are run annually
- ISO27001 Certification process is scheduled to begin in Q3 2018

Article 33 - Notification of a personal data breach to the supervisory authority

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

In the event of a personal data breach, we will aid in the notification from the Controller to the Supervisory Authority with a communique regarding the event within 72 hours of its discovery.

Article 37 – Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:
   1. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
   2. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
   3. the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

Better Impact's DPO is Kate Saunders – kate@betterimpact.co.uk - 020 3014 0226 x152

Article 44 - GDPR General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Better Impact Inc. (of Canada) is contractually obligated to Better Impact Software Ltd (of the UK) to apply all relevant provisions of the Regulation.

Article 45 - GDPR Transfers on the basis of an adequacy decision

A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country… in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.

The Commission has decided that Canada ensures an adequate level of protection and all data stored in Better Impact software is stored in Canada so no special authorisation is required. Support offered from Better Impact team members in Australia and the USA is, by default, limited to support where access to the data is not required but can be provided to organisation upon their request and at their determination of associated GDPR compliance.