Local Trust | Big Local

General Data Protection Regulation (GDPR)

Information for Big Local areas

The EU General Data Protection Regulation (GDPR) came into effect on 25 May 2018.

Each individual organisation is responsible for the data under its control. Local Trust has reviewed its data protection policies and procedures to ensure they meet the GDPR requirements and has advised its partners to do the same. This document describes the main principles of the GDPR and how it affects your Big Local partnership and relationships with Local Trust, your locally trusted organisation and your community.

What is the GDPR?

The GDPR replaced the 1995 EC Data Protection Directive and introduced new requirements for the processing of personal data. In the UK, a new Data Protection Bill incorporating the provisions of the GDPR has replaced the existing Data Protection Act.

If your Big Local partnership holds personal data about individuals, including volunteers, members of your community, residents and others, you should be aware of the GDPR's requirements and consider the steps you might take to ensure compliance.

The key data protection principles in the GDPR are similar to those in the current Data Protection Act. The major difference between the GDPR and the old data protection regime are the provisions for accountability. Whereas the current law is based on a 'checklist' approach to data protection, the new law is designed to make data controllers more accountable for their data processing activities. This means that data controllers must maintain an overview of their data processing activities, be sure that they have a legitimate basis (valid reason) for processing the data, and, where necessary or appropriate, introduce specific policies and practices that meet the GDPR requirements.

What is personal data?

Personal data is any information that can be used to identify a person. This could be a name, photograph, address, phone number or email address. It is important to remember that personal data can be held electronically, but it may also be held in other forms, such as paper, photographs, etc. The GDPR applies to all of your personal data processing activities and everyone whose data you keep. This includes employees, volunteers, members of your community and residents, supporters and donors. These people are your "data subjects" and they have rights to seek information and redress in respect to what you do with their personal data.

“Special categories” of personal data – formerly known as “sensitive data” – includes information concerning an individual’s race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for identification purposes), health, sex life or sexual orientation.

“Data processing” means just about anything that you may do with the data, including collecting or receiving, recording, storing, consulting, sharing, backing-up, updating, sending, deleting etc.

What are the key data protection principles in the GDPR?

The GDPR requires that personal data must be:

- **Processed lawfully, fairly and in a transparent way**. This means you must have a legitimate basis (valid reason, see below) for holding the data, and that its processing is both understandable to and in line with the reasonable expectations of the data subject.
- **Collected for a specific purpose and not further used in a way that is incompatible with this purpose**. This means you should only process the data for the purposes for which you collected it.
- **Adequate, relevant and limited to what is needed in relation to the purposes for which it is used**. This means you should not collect more data than you need.
- **Accurate and, where necessary, kept up to date**. This means you should take reasonable steps to ensure that your data is accurate and rectify any mistakes.
- **Kept in a form which does not allow a person to be identified for longer than is necessary**. This means that you should delete (or, if you need it for record-keeping purposes, archive) data that you no longer need for the purpose you collected it.
- **Processed in a way that makes sure personal data is kept secure, including protection against accidental loss**. This means that access to data should be restricted on a “need to know basis”. The level of security should be commensurate to the risk to the data subject of unauthorised access. Special categories of data should be subject to a high level of data security.

When can I process personal data in accordance with the GDPR?

To be compliant with the GDPR, organisations or groups must ensure that they have at least one legitimate basis or valid reason for using or processing the personal data they are holding. These include (but are not limited to):

- **Consent** from the person whose data you use or process (for consent to be valid the data subject must be fully informed of the envisaged data processing activities and have clearly indicated their consent).
- **A contract or service level agreement** with a data subject that requires you to process their personal data in order to fulfil contractual obligations or provide the specified services
- **A legal obligation** (for example the maintenance of financial records for possible inspection by tax authorities or measures concerning the safeguarding of children).
- **A “legitimate interest”** in processing the data on the part of the controller (this is the most flexible basis for processing and is likely to be most appropriate where you use people’s data in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing).

While it is often assumed that “consent” is the only or most important legitimate basis for processing personal data, the other legal bases are actually much more widely used in practice. For the GDPR, consent is particularly important where you intend to contact people repeatedly to provide information about and/or “market” your services. In these instances, you should seek the clear and unambiguous consent of the data subject to receive such communications.

What are data subjects’ rights?

The GDPR also extends the rights of those whose personal data you hold to access their information, withdraw their consent or object to the processing, and to request the correction or deletion of inaccurate or obsolete data. In simple terms, this means people can make requests at any time to check what data you hold and what you do with it, and that you are under a legal obligation to respond. If the data subject is unhappy with your response, they have the right to seek redress from a regulator (in the UK this is the Information Commissioner’s Office).

“Data controller” or “data processor”: who is responsible for what?

Under the GDPR, the “data controller” is the legal person who (either alone or in common with others) decides the purposes for which and how any personal data is processed. A “data processor” is an individual or entity that processes the data on behalf of a data controller. The GDPR places legal obligations on both the data controller and the data processor and distinguishing between the two is important in establishing lines of accountability. As a controller you must ensure that your contracts with processors meet the standards of the GDPR; as a processor you may be legally liable for any data breaches.

Local Trust has reviewed its data processing activities and relations with partners and service providers to ensure that it complies with the GDPR. While Local Trust is not responsible for the data processing activities of its Big Local partnerships or locally trusted organisations, it does expect individuals and organisations collecting personal data in the course of their Big Local work to comply with the GDPR.

What can I do to ensure I comply?

As a “data controller” it is your responsibility to comply with the GDPR and to seek assurance that any data processors you engage also comply with the GDPR. To meet your responsibilities under the GDPR you (as the partnership or locally trusted organisation) may wish to:

- **Compile an inventory of how you process data** in order to identify the legitimate basis and specific purposes for which you use personal data and the locations in which it is stored and accessed
- **Review the security of the information** to ensure that all of the personal data you process is adequately protected from others
- **Review your data management and consent procedures** to ensure that, for example, your volunteers and subscribers are aware of what data you collect and how you use it, and are happy for you to process their data in this way
- **Check that any data processors that you use are GDPR compliant**

- If you are collecting large amounts of personal data, or processing sensitive ("special categories" of) information, **establish a basic data protection policy or standard operating procedures** to ensure that the data is securely stored and that those with access to it are aware of their legal responsibilities
- **Delete or securely archive data that that you no longer need** GDPR to actively process in order to achieve the specific purpose that you collected it for
- **Check that you are in a position to respond to a subject access request** by being able to identify and locate of all of the personal data under your control

We recognise that the new regulation means you might decide to delete the data you have because it does not comply with GDPR. If this is the case you will need to consider how to ensure you comply in the future.

Where can I find further information about how to comply?

- The Information Commissioner's Office (ICO) has issued guidance for not-for-profit organisations: https://ico.org.uk/for-organisations/charity/ and for small business: https://ico.org.uk/fororganisations/business/
- The Charity Finance Group (CFG) has published a guide to help voluntary organisations comply with the EU General Data Protection Regulation (GDPR): https://cfg.org.uk/gdprguide
- The National Council for Voluntary Organisations (NCVO) has also produced guidance on the GDPR: https://www.ncvo.org.uk/practical-support/information/data-protection
- The European Center for Non-Profit Law (ECNL) has produced a guide to the GDPR's impact on fund-raising activities: http://ecnl.org/data-protection-fundraising/

This document will be developed over time with input from the people using this material.

If you have thoughts on how this document can be made more useful for you, particularly if you live in one of the Big Local areas, please let us know.

Local Trust

020 3588 0565

info@localtrust.org.uk

www.localtrust.org.uk

The endowment for the Big Local programme is held by the Big Local Trust and overseen by Local Trust. The Big Local Trust was established by the National Lottery Community Fund with a National Lottery grant of £196,873,499.

If you need this document in other formats or a community language please get in touch with Local Trust and we will help you.

Published by Local Trust in 2015, updated May 2019.

Local Trust company no. 7833396, charity number 1147511

Big Local Trust charity number 1145916