****

**Data Protection (GDPR)**

**The new legislation**

On 25 May 2018, data protection law changed with the introduction of the European General Data Protection Regulation (GDPR). It is a significant change for all organisations that hold and process personal data. The changes do not just affect big businesses; Voluntary and community organisations also need to ensure they are complying with the requirements. Privacy and data policies should be reviewed in order to be compliant with the new and more stringent regulatory framework. GVA can provide help and support with this, including template policy documents.

Brexit will not affect the introduction of this legislation as the Government plans to incorporate GDPR into UK law. So if you aren’t already compliant, don’t delay!

**Impact of GDPR**

The GDPR affects voluntary and community organisations in one way or another.

If your organisation holds personal data on **anyone**, including service users and beneficiaries, members, donors and supporters, employees and volunteers this legislation applies to you.

It includes **all types of data** whether in the form of contact information or any other sort of personal data e.g. information about ethnicity, religious belief, or bank account or credit card information.

**What is different?**

A lot of what’s in the GDPR mirrors current law under the Data Protection Act 1998 and guidance published by the [Information Commissioner’s Office](https://ico.org.uk/) (ICO). However, GDPR also introduces some new rights and obligations and makes changes to some existing concepts.

Many of the regulations in the GDPR are designed to promote increased transparency and accountability. The legislation demands more rigorous and accountable data practices. Whilst not an exhaustive list some of the key differences to be aware of are:

* **increased enforcement powers:** maximum fines of up to €20 million (that’s around £17.5 million) or 4% of total annual worldwide turnover of the preceding year, whichever is higher
* **extended geographical scope:** non-EU businesses will be subject to the regulation if they provide their service to EU organisations or monitor the behaviour of EU residents
* **Consent:**more rigorous criteria will be applied to obtaining individuals’ consent. It must be freely given, specific, informed and unambiguous e.g. fundraising consent may not be valid if it is given when grouped with non-fundraising matters
* **opt-in:** crucially, where consent is involved, you must gain explicit, opt-in consent
* **profiling:**individuals will have the right to object to profiling, which includes most forms of online tracking and wealth screening
* **the right to be forgotten:**individuals will have the right to request that you delete all their personal data
* **enhanced individual rights:** individuals will have enhanced rights with new provisions covering the right to access data (replacing subject access requests), the right to be forgotten (the right to request that an organisation delete all their personal data) and the right to data portability
* **reporting obligations**: you will also have a duty to report certain types of data breach to the ICO and, in some cases, to the individuals affected

**Things to do:**

* **Awareness**-You should make sure that decision makers and key people in your organisation are aware of the changes brought about by GDPR.

They need to appreciate the impact the new legislation has.

* **Information you hold** - You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.
* **Individuals’ rights** - You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
* **Lawful basis for processing personal data** - You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.
* **Consent** - You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don’t meet the GDPR standard.
* **Data breaches** - You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.
* **Data Protection Officers** - You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation’s structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

**Good to know:**

What does ‘**datacontroller’** mean?

A data controller decides how and why data is used

What does ‘**data processor’** mean?

A data processor is any person that processes data on behalf of the data controller (other than an employee of the data controller) such as a group secretary or admin volunteer.

* Further information/ Example for Data Controller & Processor

**Further Information:**

The ICO is the UK regulator responsible for interpreting and enforcing GDPR. Their website is the best place to start if you want more information about the GDPR.

1. [ICO - Guide to the General Data Protection Regulation (GDPR)](https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr)
2. [Resource Centre - Data Protection for community Groups](https://www.resourcecentre.org.uk/information/data-protection-for-community-groups/)
3. [NVCO about Data Protection](https://www.ncvo.org.uk/practical-support/information/data-protection)