DATA PROTECTION POLICY

Last reviewed: March 2022

Purpose

Integrity Action takes the security of its data very seriously, and seeks to manage and protect stakeholders' personal data in accordance with best practice.

All organisations are required to not only comply with but to demonstrate their compliance with the Data Protection Act 2018 (DPA 2018). The DPA 2018, it sets out requirements for how organisations must handle personal data and is similar to the European GDPR legislation.

Non-compliance risks a variety of enforcement actions including fines of up to 4% of turnover or EUR 20 million, whichever is higher for the most serious offences. One of the biggest risks of any enforcement action is reputational damage and loss of trust.

This document explains the requirements of the data protection laws and explains how Integrity Action complies.

Application

This policy applies to the processing of personal data in manual and electronic records kept by Integrity Action. It also covers Integrity Action's response to any data breach and other rights under the General Data Protection Regulation.

This policy applies to the personal data of job applicants, existing and former employees, apprentices, volunteers, placement students, workers and self-employed contractors. These are referred to in this policy as relevant individuals.

Integrity Action makes a commitment to ensuring that personal data, including special categories of personal data and criminal offence data (where appropriate) is processed in line with GDPR and domestic laws and all its employees conduct themselves in line with this, and other related, policies. Where third parties process data on behalf of Integrity Action, Integrity Action will ensure that the third party takes such measures in order to maintain Integrity Action's commitment to protecting data. In line with GDPR, Integrity Action understands that it will be accountable for the processing, management and regulation, and storage and retention of all personal data held in the form of manual records and on computers.

The personal data held by Integrity Action and the retention policy for each type of data is documented in Appendix Two. We audit the personal information held regularly.

We recognise that a significant amount of data we collect and process is not "personal data" as defined by the GDPR and DPA 2018, as such data relates to individuals not located in the EU. However, our intent is to use reasonable efforts to apply the GDPR principles to such individuals to ensure fairness and consistency.

DATA PROTECTION POLICY

Last reviewed: March 2022

Ownership

The PDA 2018 and GDPR does not require Integrity Action to formally designate a Data Protection Officer (DPO) therefore we don't have one in a formal sense. However, the Technology Manager has responsibility for overseeing data protection and GDPR compliance.

Data protection principles

All personal data obtained and held by Integrity Action will:

- be processed fairly, lawfully and in a transparent manner
- be collected for specific, explicit, and legitimate purposes
- be adequate, relevant and limited to what is necessary for the purposes of processing
- be kept accurate and up to date. Every reasonable effort will be made to ensure that inaccurate data is rectified or erased without delay
- not be kept for longer than is necessary for its given purpose
- be processed in a manner that ensures appropriate security of personal data including protection against unauthorised or unlawful processing, accidental loss, destruction or damage by using appropriate technical or organisation measures
- comply with the relevant GDPR procedures for international transferring of personal data.

In addition, personal data will be processed in recognition of an individuals' data protection rights, as follows:

- the right to be informed
- the right of access
- the right for any inaccuracies to be corrected (rectification)
- the right to have information deleted (erasure)
- the right to restrict the processing of the data
- the right to portability
- the right to object to the inclusion of any information
- the right to regulate any automated decision-making and profiling of personal data.

Procedures

Integrity Action has taken the following steps to protect the personal data of relevant individuals, which it holds or to which it has access:

1. it gave responsibility to one member of staff for:
    a. the processing and controlling of data

   b. the comprehensive reviewing and auditing of its data protection systems and procedures
   c. overviewing the effectiveness and integrity of all the data that must be protected.
2. it provides information to its employees on their data protection rights, how it uses their personal data, and how it protects it. The information includes the actions relevant individuals can take if they think that their data has been compromised in any way.
3. It provides its employees with information and training to make them aware of the importance of protecting personal data, to teach them how to do this, and to understand how to treat information confidentially.
4. It can account for all personal data it holds, where it comes from, who it is shared with and also who it might be shared with.
5. It carries out risk assessments as part of its reviewing activities to identify any vulnerabilities in its personal data handling and processing, and to take measures to reduce the risks of mishandling and potential breaches of data security. The procedure includes an assessment of the impact of both use and potential misuse of personal data in and by Integrity Action.
6. It recognises the importance of seeking individuals' consent for obtaining, recording, using, sharing, storing and retaining their personal data, and regularly reviews its procedures for doing so, including the audit trails that are needed and are followed for all consent decisions. Integrity Action understands that consent must be freely given, specific, informed and unambiguous. Integrity Action will seek consent on a specific and individual basis where appropriate. Full information will be given regarding the activities about which consent is sought. Relevant individuals have the absolute and unimpeded right to withdraw that consent at any time.
7. it has the appropriate mechanisms for detecting, reporting and investigating suspected or actual personal data breaches, including security breaches. It is aware of its duty to report significant breaches that cause significant harm to the affected individuals to the Information Commissioner, and is aware of the possible consequences.
8. It is aware of the implications of international transfer of personal data.

Access to data

Relevant individuals have a right to be informed whether Integrity Action processes personal data relating to them and to access the data that Integrity Action holds about them. Requests for access to this data will be dealt with under the following summary guidelines:

- Integrity Action will not charge for the provision of data unless the request is manifestly unfounded, excessive or repetitive, or unless a request is made for duplicate copies to be provided to parties other than the employee making the request
- Integrity Action will respond to a request without delay. Access to data will be provided, subject to legally permitted exemptions, within one month as a maximum. This may be extended by a further two months where requests are complex or numerous.

- Relevant individuals must inform Integrity Action immediately if they believe that the data is inaccurate, either as a result of a subject access request or otherwise. Integrity Action will take immediate steps to rectify the information.

For further information on making a subject access request, employees should refer to our subject access request policy, available from the Technology Manager.

Data disclosures

Integrity Action may be required to disclose certain data/information to any person. The circumstances leading to such disclosures include:

- any employee benefits operated by third parties
- disabled individuals - whether any reasonable adjustments are required to assist them at work
- individuals' health data - to comply with health and safety or occupational health obligations towards the employee
- for Statutory Sick Pay purposes
- HR management and administration - to consider how an individual's health affects his or her ability to do their job
- the smooth operation of any employee insurance policies or pension plans.

These kinds of disclosures will only be made when strictly necessary for the purpose.

Data security

Integrity Action adopts procedures designed to maintain the security of data when it is stored and transported. More information can be found in the Data transfer security policy.

In addition, employees must:

- ensure that all files or written information of a confidential nature are stored in a secure manner and are only accessed by people who have a need and a right to access them
- ensure that all files or written information of a confidential nature are not left where they can be read by unauthorised people
- check regularly on the accuracy of data being entered into computers
- always use the passwords provided to access the computer system and not abuse them by passing them on to people who should not have them
- use computer screen blanking to ensure that personal data is not left on screen when not in use.

Personal data relating to employees should not be kept or transported on laptops, USB sticks, or similar devices, unless authorised by the Technology Manager. Where personal data is recorded on any such device it should be protected by:

- ensuring that data is recorded on such devices only where absolutely necessary
- using an encrypted system — a folder should be created to store the files that need extra protection and all files created or moved to this folder should be automatically encrypted
- ensuring that laptops or USB drives are not left lying around where they can be stolen.

Failure to follow Integrity Action's rules on data security may be dealt with via Integrity Action's disciplinary procedure. Appropriate sanctions include dismissal with or without notice dependent on the severity of the failure.

International data transfers

Integrity Action does not transfer personal data to any recipients outside of the EEA.

Rights requests

We must deal with all requests within one month.

If you get a request for personal data, to correct, delete, restrict or export data, or any correspondence where an individual objects to us processing their data, send the request to the Technology Manager. They will coordinate identification of the information which needs to be provided/deleted. The CEO must review and approve all documents provided and deletions where these have been requested.

Data Protection Impact Assessment (DPIA)

Data protection issues must be considered at the planning stage of all new projects to determine if a DPIA is necessary. Wherever a project involves processing that is likely to result in a high risk to individuals, this will be obligatory. The DPIA screening checklist on the ICO website should be used to help determine whether a DPIA is necessary where this is unclear.

If it is required the template on the ICO website should be used.

In 2019 the only DPIA required was in relation to the development of DevelopmentCheck. This can be found in the GDPR folder on googledrive: Finance Team folder\Standing data\GDPR\FY19

Privacy notices

A privacy notice explains at the point of data collection what users can expect will happen to their data.

If you collect personal data you must tell the person the following information:

- how you intend to use their data;
- the lawful basis for processing that data;
- where the basis is legitimate interests, what those interests are;
- where the basis is consent that they can withdraw it at any time, and how to do so;

- who else will receive or access the data (if anyone);
- if applicable, that you intend to transfer the data outside the UK and how you made that transfer compliant;
- your data retention periods;
- the rights individuals have and that they have a right to complain to the ICO if they think there is a problem with the way we are handling their data;
- If you get data on the individual from anywhere else, the source of that data;
- Whether providing the personal data is a statutory or contractual requirement, as well as whether the individual is obliged to provide the personal data and the possible consequences if they don't provide it;
- If applicable, the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual;
- How to contact us.

It must be clear that Integrity Action is collecting the data. The information must be provided in concise, easy to understand and clear language.

Integrity Action's privacy notice is included on the website. Reference to its location should be included on job adverts so that job applicants know how their data will be used.

Data breaches and breach notification

If you think that there may have been a breach of this data protection policy, or you come across any other issue or incident affecting security or personal data, you must tell the Technology Manager and/or the CEO as soon as possible. They will prepare a response plan, investigate the potential breach and report it to the appropriate authorities and/or affected individuals if necessary. Reporting to the ICO, if required, must take place within 72 hours of us becoming aware of the breach.

Breaches include, but are not limited to:

- sending an email containing personal data (either in the email or an attachment) to the wrong person;
- loss of a personal device (e.g. smartphone, personal computer/tablet) on which you have accessed/access to personal data;
- sharing or loss of a password to devices on which you have accessed/access to personal data.

Individuals will be informed directly in the event that the breach is likely to result in a high risk to the rights and freedoms of that individual.

If the breach is sufficient to warrant notification to the public, Integrity Action will do so without undue delay.

Staff training

The Technology Manager is trained appropriately in their role under the GDPR.

Training and awareness of this policy (covering basic information about confidentiality, data protection and the actions to take upon identifying a potential data breach) must be part of the induction process for all new staff plus any volunteers, trustees and contractors who have access to personal data.

Any updates to this policy should be made aware to all staff and further training should be carried out where this is appropriate to help to ensure complete understanding and ongoing accountability and compliance.

All employees who need to use the computer system are trained to protect individuals' private data, to ensure data security, and to understand the consequences to them as individuals and Integrity Action of any potential lapses and breaches of Integrity Action's policies and procedures.

Further information (see also the IT security policy)

Information Commissioners Office (ICO)
https:\\www.ico.org.uk https://ico.org.uk/for-organisations/charity/charities-faqs/

Charity Finance Group (CFG)
http:// bit.ly/recordmanagement Record management in charities: A toolkit for improvement
http://www.cfg.org.uk/resources/Publications/~/media/Files/Resources/CFDG%20Publications/CFG266_GDPR.pdf

Institute of Fundraising
https://www.institute-of-fundraising.org.uk/guidance/research/get-ready-for-gdpr/spotlight-series/

Data Protection Network
https://www.dpnetwork.org.uk/
Has a useful template for a legitimate interests balancing test.

Taylor Wessing Global Data Hub
https://globaldatahub.taylorwessing.com/
Useful tools, checklists and general information

Law firms with free blogs/newsletters:

- Hogal Lovells
- Fieldfisher
- Taylor Wessing
- Morrison Foerster
- Bird&Bird
- Hunton Andrews Kurth
- CMS (Law Now)

Appendix One - Data protection requirements and definitions

Lawful basis for processing – non sensitive data

There are six lawful bases for processing non-sensitive data. We must determine and document the lawful basis before the processing starts. This is done in Appendix Two. We should not swap to a different lawful basis at a later date without reason and in particular cannot usually switch from consent to some other basis.

1) **Consent**: clear, freely given, informed, recorded, able to be withdrawn as easily as it was given, unambiguous and for a specific purpose.
2) **Contract**: necessary to fulfil the contract with that person, including processing necessary to deliver the product or service they have requested or that we are providing.
3) **Legal obligation**: processing is necessary to comply with a legal obligation we have (e.g. to the Charity Commission, HMRC, Companies House).
4) **Vital interests**: processing is necessary to protect someone's life (generally only used in emergency situations).
5) **Public task**: processing is in the public interest (generally used by the public sector for their official tasks).
6) **Legitimate interests**: processing is necessary for the legitimate interests of the organisation and where the interests and rights of the individuals do not override the organisation's interests. This requires us to carry out a balancing test. We will be unlikely to be able to use this lawful basis for processing that would not be in line with people's reasonable expectations and would have an unreasonable or unwarranted impact on them, or would lead to risks we cannot mitigate.

Integrity Action is a **data controller** not a data processor. A **data controller** determines the purposes and means of the processing of personal data. **Data processors** process personal data on behalf of the controller. Processing means anything that is done to, or with, personal data (including simply collecting, storing or deleting those data). **Data processing** is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Personal data is any information relating to an identified or identifiable natural person, who can be directly or indirectly identified from that information, for example, a person's name, identification number, location, online identifier. It can also include pseudonymised data. The law uses the term **data subject**.

An **identifiable person** is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that person. It includes **opinions** expressed about an individual and IP addresses (which are often collected by websites and mail houses).

Special categories of personal data is data which relates to an individual's health, sex life, sexual orientation, race, ethnic origin, political opinion, religion, and trade union membership. It also includes genetic and biometric data (where used for ID purposes).

Criminal offence data is data which relates to an individual's criminal convictions and offences.

The lawful processing of special category data requires a lawful basis **and** must meet a separate condition for special category data processing.

The only special category data we collect is in relation to disabilities and medical history. This is collected so that we can monitor the accessibility of our work and to enable us to monitor and report on inclusivity. This data collection is necessary for health and social care purposes as defined under the Data Protection Act, i.e. for assessing the working capacity of employees.