Data Protection policy and procedures

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 compliance with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA 2018).

GDPR is a Europe-wide law that applies directly and together with the DPA 2018. It sets out requirements for how organisations must handle personal data.

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.

Ownership

The 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 Head of Finance and Resources has responsibility for overseeing data protection and GDPR compliance.

Integrity Action policy and procedures

This policy applies to all data whether it is held electronically or in paper form.
However, Integrity Action aims to be a paperless office. If a paper document containing personal data is received it should be scanned, saved on google drive and disposed of securely.

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 annually.

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.

Principles set out in the GDPR

Personal data must be:

1) Processed lawfully, fairly and transparently;
2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);
3) Adequate, relevant and limited to what is necessary (data minimisation);
4) Accurate and kept up to date;
5) Kept no longer than necessary (storage limitation);
6) Processed securely to prevent unauthorised or unlawful processing, accidental loss/destruction/damage.
7) Protected by suitable accountability provisions, i.e. the controller, and processor as applies, are responsible for compliance with GDPR, and for demonstrating their compliance.

We must ensure that controls are applied to data which is extracted from DevelopmentCheck. E.g. all data relating to a project must be saved in Googledrive in the folder for that project. This ensures that it can be easily identified and deleted at the appropriate time in line with our retention policy.

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 Head of Finance and Corporate Services. 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

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 Head of Finance and Corporate Services 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. smart phone, 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.

Staff training

The finance team keep a log of who has been trained and when.

Training and awareness of this policy 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.

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 d**ata 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).

Personal data is any information relating to an identified or identifiable natural person. 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 category data is information relating to:

- racial or ethnic origin;
- political opinions;
- religious beliefs or philosophical beliefs;
- trade union membership;
- health (physical or mental health or condition);

- sex life or sexual orientation;
- genetic data; or
- biometric data (for the purpose of uniquely identifying a person).

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.

Appendix Two

What personal data do we hold?

Class of data	Personal data held	Special category data / sensitive data?	Reason for holding data Who shared with (i.e. data processors)	Lawful basis for processing	Where held?	Policy re data retention	Notes/questions/to do
Monitors (includes both adults and children)	Name Gender Age Disability Attendance at workshops/events	Disability (Y/N, not detail of what it is)	Monitoring and Evaluation, donor reporting, impact assessment. Young Innovations and Cloud Enterprise have access to this data	n/a (as not subject to GDPR)	Development Check, googledrive	Until 7 years after the end of the grant or project	Monitors are not subject to GDPR as they are not located in the EU
Partners' employees	Name Email address, Attendance at workshops/events	None	Relevant communication in relation to our work with them.	n/a (as not subject to GDPR)	Googledrive (Operations team contacts spreadsheet), Email	Until 7 years after the end of the grant or project	Partners are not subject to GDPR as they are not located in the EU
Staff	HR records – filed on googledrive in restricted access folder CV, cover letter Address Telephone number Next of kin Passport details Nationality Salary	Disability Criminal conviction, Nationality Medical and sickness history	To pay pension contributions. Data is shared with our pension provider (NEST) – name, salary. Data is provided on-line To calculate tax, NI and other	Contract Legal obligation for right to work checks and some health and safety information Employment, Social Security and Social	Googledrive, Email	7 years after contract ends	NB the time limit is based on the statutory limit for bringing a claim for breach of contract of 6 years

Class of data	Personal data held	Special category data / sensitive data?	Reason for holding data Who shared with (i.e. data processors)	Lawful basis for processing	Where held?	Policy re data retention	Notes/questions/to do
	Performance appraisal Medical and sickness history Emails sent/received on work account References Credit references given Bank account details		payroll deductions. Data is shared with our payroll provider (Buzzacott) – name, salary, NI number - by email. Reports are received via an online system.	Protection (condition for processing of special category data given in the DPA). Consent (condition for criminal offence data processing given in the DPA).			
Job applications	CV Cover letter	None	Keep unsuccessful applications/CVs in case applicants apply for a different role/appointee leaves soon after starting	Legitimate interest	Google drive, Charity jobs account	6 months from appointment of chosen candidate. For the successful candidate details will be kept for 7 years after their contract ends	
Financial records	Suppliers, contractors and donors. Bank details and address. Details of transactions undertaken with them (e.g. invoices/disbursement requests, agreements)	None	To enable efficient financial processing and to provide a clear audit trail to donors and the organisation's auditors. Not shared with	Legal obligation and contract	GMS and google drive until 30 September 2017. Google drive from 1 October 2018. No personal details are	11 years after provision of goods/services	The time period is determined by our funders i.e. Sida requires us to retain all records for 7 years after their final payment (and their grant lasts for 4 years so the maximum time we need to keep records is 11 years)

Class of data	Personal data held	Special category data / sensitive data?	Reason for holding data Who shared with (i.e. data processors)	Lawful basis for processing	Where held?	Policy re data retention	Notes/questions/to do
			anyone.		entered into Aqilla, only supplier name, amount paid/received and purpose.		
Professional contacts	Email, plus potentially Phone Social media URLs Organisation address	None	To get in touch about projects, ideas etc	Legitimate interest	Currently email accounts, business cards, could be in a database eventually	7 years	We are reviewing whether to implement a contact management system – data protection will be considered as part of this if it goes ahead
Board members	Name, address, other Board positions Board minutes – include trustees in attendance, other ad hoc information	Disability Criminal conviction, Nationality	To be able to demonstrate good governance. May be provided to auditors, Companies House, Charity Commission	Contract Employment, Social Security and Social Protection (condition for processing of special category data given in the DPA). Consent (condition for criminal offence data processing given in the DPA).	Googledrive	7 years after resignation as trustee	
Trusts and	Usually none but a trust	None	To approach for	Legitimate	Spreadsheet of	7 years	

Class of data	Personal data held	Special category data / sensitive data?	Reason for holding data Who shared with (i.e. data processors)	Lawful basis for processing	Where held?	Policy re data retention	Notes/questions/to do
foundations	might have an individual representing them		funding	interest - They have made their details public so that they can be contacted for funds	trusts		
Website cookies	TBC	None	Website analytics	Consent	TBC	TBC	TBC by the website developer

Appendix Three

Information held in DevelopmentCheck (2019 version)

- First name
- last name
- date of birth
- age range
- gender
- disability (yes/no)
- userid
- password
- email address

Information held in DevelopmentCheck (pre 2019 version = legacy system to be migrated by end 2019)

- Partner organisation
- First Name
- Last name
- Email
- Username
- Password
- Language
- Gender
- Date of Birth
- Occupation
- Profile Picture

In addition, the beneficiary survey includes:

- Are you: Male, Female, Other
- How old are you? Child (under 12), Youth (12-24), Adult (25-60), Senior (over 60)
- Do you consider yourself to have a disability? Yes, No
- Are you now or in future going to benefit from this project? Yes, No, Don’t know
- Were you, or someone you know, involved in the design or implementation of this project? Yes, No
- Are you satisfied with the way this project works? Yes, No
- Is this a useful project for your community? Yes, No, Don't Know

In the quote from a beneficiary we ask:
Name, gender, age and for a photo.

Information held in SindhupalCheck (legacy system – to be migrated by end 2019)

1. Caste
2. Ethnicity
3. Disability
4. What they do for a living
5. How many family members work for an earning
6. How much their family earns every month
7. If they have a telephone (and if it is a smartphone)
8. If they use it for internet
9. If they have access to radio/tv/ newspaper

The household survey asks:

1. number of household members
2. who the head of the household is (e.g. male/female/young/old)
3. in what work did the male spouse work the most in the last seven days
4. the number of bedrooms a residence has
5. the main construction material of their house
6. what the roof is made of
7. what type of stove they use for cooking
8. what type of toilet is used in the household
9. if the household owns other land

These questions are used to calculate the Poverty Perception Index of a beneficiary.