IMPACTFUL GOVERNANCE
Community Interest Company

Data Protection, Retention, Privacy & Confidentiality Policy 2020

Introduction

Confidentiality is central to the implementation of the core values which Impactful Governance - Community Interest Company requires all "staff" (Consultants, volunteers and contractors) to apply in all areas of their work.

In maintaining these values it is essential that information about people is respected and contained, held and used appropriately. This policy has been developed in line with the Data Protection Act (1998) and in no way limits any rights under the Freedom of Information Act (2000).

All staff, Consultants and Volunteers are required to sign the confidentiality agreement (Appendix A) during induction and before commencing any work for or with Impactful Governance - Community Interest Company.

Aim

The aim of this policy is to ensure that employees are aware of their responsibilities in maintaining confidentiality in terms of updating and storing records, access to records and disclosure of information. The contents of this policy are in line with the requirements of the Data Protection Act (1998) the Care Standards Act (2000), Supporting People Frameworks and OFSTED or other accreditation requirements.

GDPR

New regulations on General Data Protection Registration (GDPR) came into force in May 2018 and new rules apply to this policy regardless of it being updated with new laws. The Data Controller is Andrew Waite (Chief Executive) and can be contacted at Impactful Governance – Community Interest Company Office:

The Old Free School
George Street, Watford
Hertfordshire WD18 0BX

Security of Equipment and data

Impactful Governance subscribes to Kaspersky Internet Security which checks all websites and documents before opening. These are downloaded onto the Office Computer and both Directors' mobile phones. Consultants are advised to install software protection onto their own personal mobile phones and computers, especially when handling data through email communication from Impactful Governance. To limit the number of documents at risk, we use Hubspot CRM to hold client data and documents. This is where documents should be exchanged whilst held securely on a cloud-based system.

Direct Marketing & Communication
Postal mailing or electronic mailing may take place from time to time and data is collected through a physical registration of attendees at events or activities or held on Client Relationship Management (CRM) Management software and stored on cloud-based storage for existing and opted-in clients. Data is not transferred to any other organisation or to anyone outside of the European Union (E.U.) although data may be held securely on cloud-based systems outside of the E.U.

We do not pass on information to third parties and data is not permitted to be shared outside of Impactful Governance – Community Interest Company without the written consent of individuals. This includes names, address, telephone number, email or other methods of communication which remains confidential.

A CONFIDENTIALITY AGREEMENT IS SIGNED BY EVERY MEMBER WORKING FOR US, THAT INFORMATION WILL NOT BE SHARED.

Responsibilities

1. Maintaining and storing files and records

1.1 All personal files and records relating to people who use a service must be securely stored away when not in use and this must be carried out in line with the appropriate procedures in place for storage of files.

1.2 Files and records should only contain information that is necessary for their purpose.

1.3 Files and records must be retained for seven years after the person has ceased to receive services from Impactful Governance - Community Interest Company. After this period of inactivity the file must be destroyed in a manner that ensures confidentiality. Historic employment data for staff must be held for 15 years.

1.4 Information kept in files and records must be accurate and up-to-date.

1.5 All Impactful Governance - Community Interest Company staff are entitled to expect that personal information kept about themselves remains confidential. All personnel files and records must be kept in locked cupboards or cabinets.

1.6 Files should not be removed from Impactful Governance - Community Interest Company premises other than in exceptional circumstances and only with the prior knowledge and agreement of the appropriate Line Manager.

1.7 All electronic files and other forms of confidential information must be saved on password protected computer systems. If using iPads or laptops, a security code ***must*** be used for the device. If working in a public place or public transport being aware that someone could overlook screens or papers.

1.8 Staff members working from home must ensure that all confidential information is kept in a secure location that ensures confidentiality cannot be purposefully or inadvertently breached. This includes ensuring that personal

computers used for work purposes are password protected and that no files with personal data are consequently printed as a hard copy at home.

1.9 Profiling of individuals within an organisation is based on organisation activity, roles, types and geographic location. This is for the purpose of identifying the appropriately skilled and located Consultant to work with organisations and individuals.

2. Access to files and records

2.1 The person to whom files and records refers must be supported, according to their individual need, to have access to them if they wish.

2.2 Only staff members who have full and up to date (i.e. within the last three years) enhanced DBS clearance can have access to personal details of Impactful Governance - Community Interest Company service users, members, volunteers or employees. Access to personal files and records by staff members should be made on a need to know basis. The Managing Director may decide that some information about a person is confidential and that it should not be disclosed to the staff team but information ***must*** be disclosed to the Designated Senior Person (DSP) for safeguarding concerns. If confidential information is being passed on to other staff it must be made clear by the individual passing on this information that the information continues to remain confidential.

2.3 Relatives of people who use a service can have access to a person's files and records with the written consent of the relevant service user. Documents with shared information on other service users must be removed before access is given. A £20 administration fee applies for disclosing personal information.

2.4 Where a person has given their consent for any personal information to be disclosed to someone else, it is important to establish that their consent is informed and that they have an understanding of the possible implications of such a disclosure. If in doubt, consult with the Managing Director.

2.5 Volunteers, visitors and people not employed to support the person concerned should not have access to personal files and records. Specific information may be shared e.g. dietary preferences, issues relating to individual risk taking etc. This disclosure should take place preferably in the presence of the person concerned and with their prior consent. *(*Please see Impactful Governance - Community Interest Company*'s* Volunteer Guidelines or speak with the Managing Director*)*.

2.6 Certain people, such as the Care Quality Commission, OFSTED Inspectors, and Care Managers have legal rights to access personal information.

2.7 All Impactful Governance - Community Interest Company staff are entitled to have access to files and records kept about them by making a written request and allowing 7 days notice.

2.8 Where a person using a service has seen their file and feels that information is inaccurate in anyway, they may request that the file be amended. This

request should be made to a senior manager, stating the reasons why. People may ask team members to support them in making the request.

2.9 Where an employee has seen their file and feels that information is inaccurate in anyway, they may request that the file be amended. This request should be made in writing to the Managing Director, stating the reasons why they feel the file should be amended.

2.10 If in doubt about a person's right to access personal information, consult with a senior manager. Remember that access to confidential information will only be made on a 'need to know' basis.

2.11 Subjects are able to opt-out of correspondence and request their information to be removed at any time by confirming their request in writing by email or by post. Evidence of the individual owner will be sought to clarify the data belongs to the subject making the request.

3. Verbal Communication

3.1 Confidentiality is equally applicable to verbal information as to written information. Telephone conversations must limit the amount of information that you can give without categorically having proof of the authorised recipient. This also applies to anyone within hearing distance of a telephone conversation. In addition to the previous stipulations, the following guidance applies.

3.2 Confidentiality must be ensured when arranging meetings with people supported by Impactful Governance - Community Interest Company services. As such, meetings should only be arranged in public spaces at the explicit request of the person being supported.

3.3 Workers should avoid making work-related telephone calls outside of Impactful Governance - Community Interest Company venues or the home of the service user the telephone call relates to. If such telephones conversations must be undertaken in a public place, staff should move to the most private area available. They must also ensure that they do not use any identifying details during the course of the conversation. This includes names, addresses, dates of birth and any personal issues.

4. Disclosure of Information

4.1 Employees should be aware that there may be circumstances where they are not able to respect someone's confidentiality – these will be in situations where someone discloses that they have abused someone or are being abused or when any breach of a disciplinary rule is alleged. In these circumstances a Managing Director or DSP must be contacted. In the event that someone is being abused, the Safeguarding Policy must be followed. Also, where there is a possible breach of the Impactful Governance - Community Interest Company's disciplinary rules the Disciplinary Procedure will be instigated.

4.2 Disclosure of personal information should always be kept to an absolute minimum and on a 'need to know' basis only. When discussing matters with someone and a safeguarding issue arises, we must stop the discussion and inform the other party that a safeguarding issue will be reported to a DSP as part of a legal Duty to Report.

4.3 In deciding whether or not to disclose information, employees should consider the following points;

- Does the person to whom it is being disclosed need to know?
- Is the person aware that the information is confidential? People must be told the status of information so that they know how to treat the information.
- How can the information be conveyed in a way that is respectful, discreet and sensitive?

If in doubt, contact the DSP.

4.4 In deciding whether or not someone needs to know the information, employees should consider the following points;

- We have a legal Duty to Report all Safeguarding issues.
- We will not be putting the person at risk if we disclose the information to a DSP.
- What harm might we do by not disclosing the information?
- Do Impactful Governance - Community Interest Company colleagues need to have the information to be able to support the person adequately?
- Consider the seven conditions of Data Protection if sharing with anyone other than Safeguarding officials.

If in doubt, contact the Managing Director.

4.5 Where information regarding a service user needs to be passed on to a professional who works with that person (e.g. a Doctor, ambulance or Care provider), this will be discussed with the service user concerned beforehand.

4.6 Information about a person may be given to a relative or family member of a person living in a residential service following discussion with the person concerned and a senior manager.

4.7 Personal information about an Impactful Governance - Community Interest Company staff member should not be disclosed to another staff without their c

4.8 Personal information about an Impactful Governance - Community Interest Company staff member may need to be passed on to a manager within the service or to a senior manager if it relates to the quality of service being provided. This should be on a ‘need to know’ basis only.

A failure to adhere to this policy which results in inappropriate disclosure of confidential information is a disciplinary offence and will be dealt with in accordance with Impactful Governance - Community Interest Company’s Disciplinary Procedure, which could result in dismissal.

Data Protection, Retention and Security of Information

Impactful Governance - Community Interest Company takes the concept of **confidentiality very seriously** and does all in its power to restrict personal information to those who genuinely need to know. Breach of confidentiality will result in **disciplinary measures and removal from service, business or activity** of any person found to be in breach of our Data Protection, Retention, Privacy & Confidentiality Policy.

To comply with the principles of the Data Protection Act, Impactful Governance - Community Interest Company will endeavour to ensure that **strict confidentiality of clients' personal data is maintained in all of its work**, whether the information is stored on a computer or a manual filing system.

Impactful Governance - Community Interest Company will also ensure that:

access to personal information by its staff is on a "need to know" basis only; personal information is not given to any outside party without the consent of the person concerned (or their legal or appointed representative);

information is stored securely and can be reinstated/restored in an emergency;

clients are made aware that they have the right to request access to information concerning them for an administration fee of £20.

Clients are defined as organisations and individuals we engage with or any individual or organisation who receive a service.

All personal information will be stored under lock and key in the office and/or on computer protected by a security code. Computer held records will be copied onto a disk and stored at a designated site away from Impactful Governance - Community Interest Company's office or in a fire-proof safe within the registered office.

All clients will be made aware that they have a right to access personal information held on them, but should give reasonable notice of this request to the senior manager responsible. References will remain confidential.

Personal information about clients will be shared within Impactful Governance - Community Interest Company on a strictly "need to know" basis and will not be shared with outside agencies without the prior permission of the person concerned (or their legal or appointed representative), except in unavoidable or exceptional circumstances.

Notes of meetings with clients where personal issues are discussed will not be freely circulated or accessible and will be stored securely.

Personal data will not be kept unnecessarily and in normal circumstances will be destroyed after 5 years (please refer to Data Retention for further information).

Personal data and confidential documents will be shredded on disposal.

Adequate security precautions must be taken when laptop computers, mobile or iPads and personal data is taken out of the office, e.g. Must be passcode protected, not left unattended or kept in the boot or locked car glovebox.

The Data Protection Controller is the Chief Executive of Impactful Governance - Community Interest Company (Andrew Waite) and the Data Protection Compliance Officer is the Customer Service Director (Alexandre Oliveira).

All staff are made aware of this policy and agree to abide by it.

All papers containing client data is locked away each evening or upon leaving the office.

Freedom of Information

If a request is received for access to information under the Freedom of Information Act staff should refer the matter to the Chief Executive. In deciding whether there is a duty to disclose the information requested, the Chief Executive should consider all individual's rights of protection under the Data Protection Act.

Staff, Consultants and Volunteers are to comply with all of the Principals of Data Protection and are aware of the consequences of non-compliance.

Breaches of Data Protection are Disciplinary matters and currently carry a penalty of 1,000,000 Euro or 4% of the organisation annual turnover.

Any discovered data security breach will be notified to Information Commissioners Office within 72 hours. We will report the nature of any breach, the number of data subjects, categories of data and our proposed mitigation (see Appendix B).

Date of last review	May 2020
Date of next review	May 2021
Date it was first implemented	October 2017
Author(s)	Directors
Audience	All Consultants, Employees & Volunteers.
Other relevant policies and/or procedures	Whistle Blowing policy, Disciplinary policy, Safeguarding Policy, Confidentiality Agreement.
Where it is saved and displayed	www.ig-CIC.org.uk

Impactful Governance - Community Interest Company reserves the right to amend or revise the policy above in accordance with changes in custom and practice.

IMPACTFUL GOVERNANCE
Community Interest Company

Appendix A

Confidentiality Agreement

All persons engaged with Impactful Governance – Community Interest Company, whether as an employee, Consultant or volunteer must always be aware of the confidentiality and privacy of information and data gained by them during the course of their interactions and/or duties with Impactful Governance and our clients (see Data Protection, Retention, Privacy & Confidentiality Policy).

It is expected that employees and volunteers, working with or for Impactful Governance treat information in a discreet and confidential manner.

Particular attention is drawn to the following:

Data must not be shared with any organisation outside of Impactful Governance – Community Interest Company (See GDPR).

Written records, including computerized information and correspondence, must be kept securely at all times when being used by an authorized person.

Client data is held securely on a CRM system, accessed by authorized members of the team and cannot be exported or shared with anyone outside of Impactful Governance – Community Interest Company.

Information regarding students, delegates, parents, carers or any other individual must not be disclosed either orally or in writing to an unauthorized person or organisation at any time unless there is a partnership agreement and explicit pemission is outlined at the data collection point.

Conversations relating to confidential matters should not take place in situations where they may be overheard by passers-by, this includes when in the workplace or on placement.

Any breach of confidentiality or privacy will be considered as misconduct and the subject of serious action e.g. termination of employment and investigation by the Information Commissioners Office.

The importance of confidentiality cannot be stressed too much and it is important to be borne in mind at all times.

I have read, understood and accept the terms of confidentiality and privacy (above).

Signed …… Printed ……..

Dated ……

Appendix B

Data Breach Reporting Form

Please complete this form to report a personal data breach to the Data Protection Officer.

This form should be read alongside our **Data Breach Process** document (below), which provides further information and key definitions before completing the Reporting Form.

Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

Report Type:

[ ]Initial report

[ ] Follow-up report

(Follow-up reports only) Directors case reference:

DATA BREACH PROCESS

The purpose of this document is to outline the process for reporting and managing data breaches. It sets out the requirements of the University to report data breaches to the Information Commissioners Office (ICO) and the action to be taken.

What is a Data Breach?

The ICO defines a personal data breach as 'the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate causes.'

- deliberate or accidental action (or inaction) by a controller or processor; sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen; alteration of personal data without permission; and
- loss of availability of personal data
- A personal data breach occurs when 'any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed'

Reporting a Data Breach

If a data breach has been identified, the Directors must be notified immediately, providing the following information:

- What the breach is (e.g. information has been accidentally sent to a third party via email)
- What information is contained/has been breached
- Whose data is involved (e.g. students, staff) and the number of individuals/personal
- data records it concerns
- Where the breach occurred
- When the breach occurred

The likely consequences of the breach Any steps already taken to mitigate the breach (if any)

You can contact the Data Protection Officer at admin@ig-cic.org.uk .

You must report the breach as a matter of urgency as Impactful Governance is required to report the breach to the ICO no later than 72 hours after the breach occurred.

Steps for reporting a breach, and required timescales

Action required Timescale (from the time the breach is identified) 1 Report the breach to your line manager and the Directors immediately

- Complete the Data Breach Reporting Form and send to one of the Directors.
- The Data Protection Officer will inform the Chief Executive within 2 hours
- Data Protection Officer will then advise the Customer Service Director
- The Chief Executive will then identify whether the breach is required to be reported to the ICO or not. This is dependent on the gravity of the breach.

Discuss the matter with the ICO on a 'without prejudice' basis.

Advise and seek instructions from the Chief Executive.

- The Directors will provide advice and guidance to the person reporting the breach within 6 hours on the steps to be taken to mitigate the breach.
- If the breach is considered 'high risk', the Directors will inform the individuals concerned in conjunction with the relevant department about the breach of their personal data within 24 hours.
- The Directors will then record the data breach within the next 24 hours and store all relevant communications on file (within 48 hours).
- Informing individuals about any breach of their data within the final 72 hours, if one is found or likely to have happened.
- If required, the Data Controller will report the data breach within 10 hours of the breach, to the ICO keeping within the 72-hour deadline and continue to liaise with them as required.

If applicable, the Customer Service Director will contact the individual/s concerned and notify them of the following:

- The name and contact details of Impactful Governance's Data Protection Officer
- A description of the likely consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach and, if applicable, the measures taken to mitigate any possible adverse effects.

Information to be reported

Any data breach should be reported to the Directors, even if it not made directly by staff at Impactful Governance – Community Interest Company (***the company***). This includes information about data breaches made by third parties the company works with, including partners and third-party system providers.

These should be reported to the Directors as a matter of urgency as above.

1. Next steps

Once the data breach has been identified and the appropriate action has been taken, the Directors will advise on the next steps to be taken and will liaise with you to identify what updates and improvements are required to ensure the breach doesn't occur again and to reduce the potential of any other data breaches in future.

2. Directors

Will review how we:

- Process personal data which could result in a risk of physical harm if there is a security breach
- Process data in a way which prevents individuals exercising a right or using a service or contract
- Participate in a new data-sharing initiative with another organization(s) or transfer personal data outside the EU Process personal data in ways which individuals might not reasonably expect
- Also consider doing a DPIA in any major project involving use of personal data, even if it is not sensitive data (e.g. if you are going to use a significant amount of personal data from a large number of data subjects). If you decide not to, document your reasons. Conduct a new DPIA if the nature, scope, context or purposes of the processing changes.

If you think it likely that a DPIA is required, contact the Data Protection Officer who can provide guidance, and may ask you to fill in a Data Protection Impact Assessment Form.

3. Step 2

Determine that the processing is necessary and proportionate

1) Describe the proposed processing and why it is being proposed. This should include an analysis of how the data will be obtained, used and retained.

2) Assess the necessity and proportionality of the processing in relation to the purpose, i.e. can it be done another way that requires less processing of personal data?

3) Always consider whether you can anonymise or at least pseudonymise the data you wish to process. You may be able to anonymise at a later date, safely destroying the original identifiable data. Also consider whether you can conduct the activity with less data either in terms of quantity or quality — only take what you need.

4. Step 3

Identify the risks associated with the processing

1) Assess the risks to the rights and freedoms of the individuals whose data is being processed, i.e. what would happen if the data was lost or misused in some way? When doing this, you need to consider the rights of individuals under the GDPR. (ICO guidance on rights of data subjects is available at: https://ico.org.uk/for- organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/. If you have any questions about this, consult the Data Protection Officer.
2) Consider the risk that the processing poses (if any) to compliance with the GDPR and to the University more broadly. ws University of Bedfordshire

Customer Service Director

5. Step 4

Identify solutions/mitigations to the risks

1) Describe safeguards and security measures put in place, privacy by design, use of data processing and data sharing agreements.
2) Consider seeking the views of the data subjects, or their representatives and other interested parties (i.e. data processors, sector specialists).

6. Step 5

Feed the results into the proposal

1) Assess if there are changes that need to be made to the proposal and define how the risks will be monitored.
2) Make sure that the solutions proposed deal with the risk. If you are not sure about acceptable levels please contact the Data Protection Officer.

7. Step 6

Approval

1) Measures and residual risks should be approved by the relevant project lead. If any residual high risks are identified, the Data Protection Officer should be informed of these (as the ICO may need to be consulted).
2) Once completed, send the DPIA form to the Data Protection Officer, who will review it, and offer advice. It will then be sent for approval to the Directors, and Data Controller.

8. Step 7

Implementation and Review

1) Once the DPIA has been approved, it is safe to proceed. Make sure that all those involved in the processing are aware of the necessary solutions.
2) Keep a record of your processing activities, and regularly review them to ensure they are still compliant with the acceptable position. Be responsive to any necessary changes.
3) Set review dates for 1 month, 3 months, 6 months, and then 12 months after the initial DPIA. Thereafter, review annually or if there is a change in how you process data (whichever is first). Inform the Data Protection Officer of any changes.

About the Breach

What has happened?

Tell us as much as you can about what happened, what went wrong and how it happened

Was the breach caused by a cyber incident?

[ ] Yes

[ ] No [ ]

How did you find out about the breach?

When did you discover the breach?

Date:

Time:

When did the breach happen?

Date:

Time:

Categories of personal data included in the breach (tick all that apply)

[ ]Data revealing racial or ethnic origin

[ ]Political opinions

[ ]Religious or philosophical beliefs

[ ]Trade union membership

[ ]Sex life data

[ ]Sexual orientation data

[ ]Gender reassignment data

[ ]Health data

[ ]Basic personal identifiers, e.g. name, contact details Identification data, e.g. usernames, passwords Economic and financial data, e.g. credit card numbers, bank details

[ ] Official documents, e.g. driving licences

[ ]Location data

[ ]Genetic or biometric data

[ ]Criminal convictions, offences

[ ]Not yet known [ ] Other (please give details below)

Number of personal data records concerned?

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

[ ]Employees

[ ]Users

[ ]Subscribers

[ ]Students

[ ]Clients

[ ]Patients

[ ]Children

[ ]Vulnerable adults

[ ]Not yet known

[ ]Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

[ ]Very likely

[ ]Likely

[ ]Neutral — neither likely nor unlikely Unlikely

[ ]Very unlikely

[ ]Not yet known

[ ]Please give details

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

[ ]Yes [ ] No

(Cyber incidents only) If you answered yes, please specify (tick all that apply)

[ ]Confidentiality

[ ]Integrity

[ ] Availability

(Cyber incidents only) Impact on the organisation

[ ]High -we have lost the ability to provide all critical services to all users

[ ] Medium — we have lost the ability to provide a critical service to some

[ ] Low -—there is no loss of efficiency, or a low loss of efficiency, and we can still provide all critical services to all users

[ ] Not yet known.

(Cyber incidents only) Recovery time

[ ]Regular — we can predict our recover time, with existing resources

[ ]Supplemented — we can predict our recovery time with additional resources

[ ]Extended — we cannot predict our recovery time, and need extra resources

[ ]Not recoverable — recovery from the incident is not possible, e.g. backups can't be restored Complete — recovery is complete

[ ]Not yet known

Had the staff member involved in this breach received data protection training in the last two years?

Yes

No

Don’t know

The breach did not involve an Impactful Governance Staff (please give details below):

(Initial reports only) If there has been a delay in reporting this breach, please explain why

(Follow-up reports only) Describe any measures you had in place before the breach with the aim of preventing a breach of this nature

Taking action Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, e.g. confirmed data sent in error has been destroyed, updated passwords, planning information security training.

(Follow-up reports only) Outline any steps you are taking to prevent a recurrence, and when you expect they will be completed

Have you told data subjects about the breach?

[ ]Yes, we've told affected data subjects

[ ]We're about to, or are in the process of telling data subjects No, they're already aware

[ ]No, but we're planning to

[ ]No, we've decided not to

[ ]We haven't decided yet if we will tell them or not

[ ]Something else (please give details below)

Details of Person making this report, in case we need to contact you for further details:

Name:

Job title:

Email:

Phone:

Please send your completed form to admin@ig-cic.org.uk with 'Personal data breach notification' in the subject field.

Data Protection Impact Assessment Form

This form should be filled out at the beginning of any major project involving:

The use of personal data, or if you are making a significant change to an existing process.

Use this form alongside our Data Protection Impact Assessment Guidance, which provides further information and key definitions to help you identify if you need to conduct a DPIA. The final outcomes of your DPIA should be integrated back into your project plan.

Details of Person completing the form:

Name: Job title:

Email:

Phone: DPIA Reference Number (Directors to fill): Type:

Initial DPIA Review (please indicate date of review): Date: ……...

Part A: Identify the need for a DPIA

1. Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

Part B: Describe the processing

2. Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or another way of describing data flows. What types of processing identified as likely high risk are involved?

3. Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much

data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

Special category data is personal data which is more sensitive and could create significant risks to a person's fundamental rights and freedoms, e.g. by putting them at risk of unlawful discrimination. Some examples are:

- Race:
- Ethnic origin:
- Politics:
- Religion:
- Trade union membership:
- Genetics; biometrics (where used for ID purposes);
- Health:
- Sex life:
- Sexual orientation:

Criminal offence data is separate from special category data, and means personal data relating to criminal allegations, proceedings, or convictions, or related security measures.

4. **Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?**

5. Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing for you, and more broadly?

Part C: Consultation process

6. **Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views - or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?**

Part D: Assess necessity and proportionality

7. Describe compliance and proportionality measures, in particular: What is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights?

What measures do you take to ensure processors comply? How do you safeguard any international transfers?

Part E: Identify and assess risks:

Describe the source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary	**Likelihood of Harm** (Remote, possible or probable)	**Severity of Harm** (Minimal significant or severe)	**Overall risk** (Low, medium or high)

Part F: Identify measures to reduce risk.

Risk	**Options to reduce or eliminate risk**	**Effect on risk** (eliminated, reduced or accepted)	Residual risk (Low, medium or high)	Measure approved Yes/No

Part G: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks Approved by:		Before accepting any residual high risk, inform the DPO, who will consult the ICO.
DPO advice provided:		DPO should advise on compliance, part F measures and whether processing can proceed
Summary of DPO advise:		
Data Controller Approval		Chief Executive to indicate approval, and any further comments/Advice
Comments:		
Registrar approval		Registrar to indicate approval, and any further comments/advise.
Comments:		

This DPIA will be kept under review by:		The DPO should also review on going compliance with DPIA

Please return your complete form to the Data Protection officer:

Finance@ig-cic.org.uk