Data Governance Policy

Version 2- June 2020

Trinity CHELTENHAM

Definitions

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not automated processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of automated processing.

Company Personnel: all employees, workers, volunteers, consultants, contractors, directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the data subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the processing of personal data relating to them.

Data Controller: the person or organisation that determines when, why and how to process personal data. It is responsible for establishing practices and policies in line with the GDPR. We are the data controller of all personal data relating to our company personnel and personal data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold personal data. Data subjects may be nationals or residents of any country and may have legal rights regarding their personal data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of privacy by design and should be conducted for all major system or business change programs involving the processing of personal data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the company data privacy team with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a data subject or information relating to a data subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal data includes special category data and pseudonymised personal data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of personal data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of personal data is a personal data breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Policies: separate notices setting out information that may be provided to data subjects when the company collects information about them.

Processing or Process: any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the company's policies, operating procedures or processes related to this Data Governance Policy and designed to protect personal data.

Special Category Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and personal data relating to criminal offences and convictions. The company also considers photographs to be special category data.

Introduction

Trinity Cheltenham is required by law to comply with the Data Protection Act 2018 (“the Act”). This Act came into force on 25 May 2018 and relates to the holding and processing of personal information.
Trinity Cheltenham needs to process personal data about individuals (“data subjects”) who are our employees, members of congregation, business contacts, suppliers and other individuals for the following purposes:

- Provision of ecclesiastical services
- HR administration
- Accounts and records

- Pastoral and spiritual care
- Information and administration

To comply with the act all data must be collected and used fairly, stored safely and not disclosed to any other person unlawfully.

This policy applies to Trinity Cheltenham, Trinity Cheltenham employees, volunteers and third parties. This policy has been adopted by the Leadership and communicated to everyone involved in our Church ensure their commitment to it.

This Data Governance Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present employees, past or present members of congregation, volunteers, supplier contacts, shareholders, website users or any other data subject.

This Data Governance Policy applies to all company personnel ("you", "your"). You must read, understand and comply with this Data Governance Policy when processing personal data on our behalf and attend training on its requirements. This Data Governance Policy sets out what we expect from you in order for Trinity Cheltenham to comply with applicable law. Your compliance with this Data Governance Policy is mandatory. Privacy policies are available to help you interpret and act in accordance with this Data Governance Policy. You must also comply with all such related policies.

Any breach of this Data Governance Policy may result in disciplinary action.

Scope

We recognise that the correct and lawful treatment of personal data will maintain confidence in Trinity Cheltenham and will provide for successful operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. Trinity Cheltenham is exposed to potential fines of up to EUR20 million (approximately £18 million) or 4% of total worldwide annual turnover, whichever is higher, for failure to comply with the provisions of the GDPR.

All areas of Trinity Cheltenham are responsible for ensuring that employees comply with this Data Governance Policy and need to implement appropriate practices, processes, controls and training to ensure such compliance.

Please contact the Operations Manager with any questions about the operation of this policy or the GDPR or if you have any concerns that this policy is not being or has not been followed. In particular, you must always contact the Operations Manager in the following circumstances:

- If you are unsure of the lawful basis which you are relying on to process personal data (including the legitimate interests used by Trinity Cheltenham);
- If you need to rely on consent and/or need to capture explicit consent;
- If you are unsure about the retention period for the personal data being processed;
- If you are unsure about what security or other measures you need to implement to protect personal data;
- If there has been a personal data breach;

- If you are unsure on what basis to transfer personal data outside the EEA;
- If you need any assistance dealing with any rights invoked by a data subject;
- Whenever you are engaging in a significant new, or change in, processing activity which is likely to require a Data Protection Impact Assessment (DPIA) or plan to use personal data for purposes other than those for which it was collected for;
- If you plan to undertake any activities involving automated processing including profiling or automated decision-making;
- If you need help complying with applicable law when carrying out direct marketing activities; and
- If you need help with any contracts or other areas in relation to sharing personal data with third parties (including our suppliers).

Data Protection Principles

We shall abide by the six data protection principles set out in the Act. These state that personal data
shall be:

- Processed lawfully, fairly and in a transparent manner;
- Processed for specified, explicit and legitimate purposes;
- Adequate, relevant and limited to what is necessary;
- Accurate and kept up-to-date;
- Kept for no longer than is necessary; and;
- Processed in a manner than ensures appropriate security.

This policy shall guide all who process data at Trinity Cheltenham to ensure that these principles are followed and any breach, whether deliberate or through negligence, may lead to disciplinary action being taken. The term ‘data’ refers to paper copies and electronic copies, and covers every form of information that we hold.

In order to meet the requirements of the principles above, Trinity Cheltenham will:

- Observe fully the conditions regarding the fair collection and use of personal data;
- Meet its obligations to specify the purpose for which personal data is used;
- Collect and process appropriate personal data only to the extent that is needed to fulfil operations or any legal requirements;
- Ensure the quality of personal data;
- Apply strict checks to determine the length of time personal data is held;
- Ensure that the rights of data subjects can be fully exercised under the Act;
- Take the appropriate technical and organisational security measures to safeguard personal data; and
- Ensure that personal data is not transferred abroad without suitable safeguards.

Person Responsible For Data

Trinity Cheltenham has appointed a person who is responsible for ensuring compliance with the Data Protection Act, implementation of this policy, Trinity Cheltenham data protection registrations and subject access requests. This person is the Operations Manager and any questions or concerns should be sent to dataprotection@trinitycheltenham.com

Employees and Volunteer Responsibilities

All employees and volunteers are responsible for:

- Complying with the six data protection principles of the Act as set out above;
- Checking that any personal data they provide to Trinity Cheltenham is accurate and up to date;
- Informing Trinity Cheltenham of any changes to information which they have provided, e.g. changes of address;
- Checking any information that Trinity Cheltenham may send out from time to time, giving details of information that is being kept and processed;
- Ensuring that personal data is not disclosed without clear authority from Trinity Cheltenham to do so;
- Complying with this policy, if, as part of their responsibilities, employees collect information about other people or personal circumstances, or about employees under their management;
- Not disclosing information they become aware of through their role;
- Informing the Operations Manager of any breaches immediately; and
- Informing the Operations Manager of any loss of data subject records immediately.

Lawfulness and Fairness

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

We shall only collect, process and share personal data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but to ensure that we process personal data fairly and without adversely affecting the data subject.

The GDPR allows processing for specific purposes, some of which are set out below:

- The data subject has given his or her consent
- The processing is necessary for the performance of a contract with the data subject
- To meet our legal compliance obligations
- To protect the data subject's vital interests
- To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of data subjects. The purposes for which we process personal data for legitimate interests need to be set out in an applicable privacy policy.

Protecting Personal Data

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data. You are responsible for protecting the personal data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised processing of personal data and against the accidental loss

of, or damage to, personal data. You must exercise particular care in protecting special category data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all personal data from the point of collection to the point of destruction. You may only transfer personal data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the personal data, defined as follows:

- Confidentiality means that only people who have a need to know and are authorised to use the personal data can access it;
- Integrity means that personal data is accurate and suitable for the purpose for which it is processed;
- Availability means that authorised users are able to access the personal data when they need it for authorised purposes; and

You must comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect personal data.

Transparency

The GDPR requires data controllers to provide detailed, specific information to data subjects depending on whether the information was collected directly from data subjects or from elsewhere. Such information must be provided through appropriate privacy policies which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand them.

Whenever we collect personal data directly from data subjects, including for human resources or employment purposes, we must provide the data subject with all the information required by the GDPR including the identity of the data controller, how and why we will use, process, disclose, protect and retain that personal data through a fair processing notice which must be presented when the data subject first provides the personal data..

When personal data is collected indirectly (for example, from a third party or publicly available source), we shall provide the data subject with all the information required by the GDPR as soon as possible after collecting / receiving the data. We shall also check that the personal data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed processing of that personal data.

Data Subject Rights

Data subjects have rights when it comes to how we handle their personal data. These include rights to:

- Withdraw consent to processing at any time;

- Receive certain information about the data controller's processing activities;
- Request access to their personal data that we hold;
- Prevent our use of their personal data for direct marketing purposes; ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- Restrict processing in specific circumstances;
- Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- Request a copy of an agreement under which personal data is transferred outside of the EEA;
- Object to decisions based solely on automated processing, including profiling (ADM);
- Prevent Processing that is likely to cause damage or distress to the data subject or anyone

else;
- Be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- Make a complaint to the supervisory authority; and
- In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

You must immediately forward any request you receive to the Operations Manager.

Data Subject Access Request

Trinity Cheltenham shall comply with data subject's right of access under GDPR.

In general terms, data subjects, including employees and members of the congregation have a right of access to personal information, the purpose for which the information is being held and to whom the information is being disclosed to. Data subjects (i.e. the individuals on whom data is held) have the right to:

- Know whether we or someone else on our behalf are processing personal information about them;
- Know what information is being processed, the reason it is being processed and those to whom it may be disclosed;
- Receive a copy of the personal information about them; and know about the source(s) of the information.

To obtain access to data, an individual must send either a written or electronic subject

access request. We shall verify the identity of an individual requesting data.

There will be no fee to provide this information. The information will be supplied in a permanent form unless this is not possible, the member agrees or there would be 'disproportionate effort' involved in its supply.

If an individual makes a request by electronic means, we shall provide its response in electronic form too (unless otherwise requested by the individual).

All requests received for access to or rectification of personal data must be directed to the Operations Manager who will log each request as it is received. A response to each request will be provided within 30 days of the receipt of the written request from the data subject.

We will be able to extend the period of compliance by a further two months where requests are complex or numerous. If this is the case, we shall inform the individual within one month of the receipt of the request and explain why the extension is necessary.

Where requests are manifestly unfounded or excessive, in particular because they are repetitive, Trinity Cheltenham can:

- Charge a reasonable fee taking into account the administrative costs of providing the information; or
- Refuse to respond.

Where Trinity Cheltenham refuse to respond to a request, We shall explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

It should be noted that situations may arise where providing the information requested by a data subject would disclose personal data about another individual. In such cases,

information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.
We shall not use personal data for new, different or incompatible purposes from those disclosed when it was first obtained unless you have informed the data subject of the new purposes and they have consented where necessary.

Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

You may only process personal data when performing your job duties requires it. You cannot process personal data for any reason unrelated to your job duties.

You may only collect personal data that you require for your job duties: do not collect excessive data. Ensure any personal data collected is adequate and relevant for the intended purposes.

You must ensure that when personal data is no longer needed for specified purposes, it is deleted or anonymised in accordance with Trinity Cheltenham's data retention guidelines. See appendix A.

Accuracy

Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

We shall ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date personal data.

Members of congregation have the ability to update their personal information using Church Suite.

Storage Limitation

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

We shall not keep personal data in a form which permits the identification of the data subject

for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

Trinity Cheltenham will maintain a record retention policy to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

We shall take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with the Trinity Cheltenham's records retention

schedule. This includes requiring third parties to delete such data where applicable.

Training

Trinity Cheltenham will provide any training of personnel necessary for the maintenance of data protection compliance at least annually.

All new starters will receive comprehensive data protection training at induction.

Transfer Limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined.

We shall only transfer personal data outside the EEA if one of the following conditions applies:

- The European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;
- Appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Operations Manager;
- The data subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or the transfer is necessary for one of the other reasons set out in the GDPR including the
- Performance of a contract between us and the data subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the data subject is physically or legally incapable of giving consent and, in some limited cases, for our legitimate interest.

Children's Data

Children are able to consent to the processing of personal data if over 13 years of age and have the same rights as an adult in relation to their data.

Where a child is under 13, consent must be sought from the person who holds parental responsibility over the child.

However, it should be noted that where processing is lawful under other grounds, consent need not be obtained from the child or the holder of parental responsibility.

Trinity Cheltenham has a youth privacy policy.

Confidential Waste

Confidential records include those that contain personal information about a living individual or are
sensitive, including, but not limited to:

- Any documentation including personal information
- Data Collection forms / 'get connected' cards
- Prayer requests
- Pastoral care and spiritual guidance notes
- Any document which reveals the contact or financial details of a named living person
- Job applications
- References
- Interview notes

There are confidential waste bins located in the office. In addition, a shredder is available for use. Staff must ensure that all special category data is treated as confidential waste and disposed of in the waste bins provided for this purpose.

Retention of Data

Trinity Cheltenham will decide on how long it retains documentation, considering the following:

- The type of work the Trinity Cheltenham does;
- The size of Trinity Cheltenham and our membership database;
- Limitation periods;
- The possibility of claims or complaints against Trinity Cheltenham, including Trinity Cheltenham's record of claims and complaints and how long these have taken to surface;

Even when a minimum period for storage of documentation has been decided upon, in many cases the decision whether to destroy documentation will need to be made on a document-by-document basis, taking into account issues such as:

- The nature and complexity involved;
- Whether the data subject was vulnerable, had a disability or was particularly difficult to deal with; and,
- Whether the member is likely to return to Trinity Cheltenham.

Record Keeping

The GDPR requires us to keep full and accurate records of all our data processing activities.

We shall keep and maintain accurate corporate records reflecting our processing including records of data subjects' consents and procedures for obtaining consents.

These records should include, at a minimum, the name and contact details of the Data Controller, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

Computer Records

Only authorised personnel will have access to specific data subject records. Electronic records will be retained securely and access will be appropriate to role and responsibility.

Request for Information

If an unauthorised third party requests information about a data subject, no information will be disclosed without prior written authority to release information from the data subject.

Responsibility of Data Subjects

All data subjects have an obligation to:

- Ensure that any information they provide is accurate and up to date
- Inform the Operations Manager of any changes to information which they have provided, e.g. changes of address
- Inform the Operations Manager of any known errors

Breaches

The GDPR requires data controllers to notify any personal data breach to the applicable regulator and, in certain instances the data subject within 72 hours.

We have put in place procedures to deal with any suspected personal data breach and will notify data subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a personal data breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the Operations Manager as the key point of contact for personal data breaches. You shall retain all evidence relating to the potential personal data breach.
If a breach occurs outside of normal office hours, you must report the breach as soon as you become aware by emailing dataprotection@trinitycheltenham.com and messaging [xxx].

Privacy By Design and Data Protection Impact Assessments (DPIA)

We are required to implement privacy by design measures when processing personal data by implementing appropriate technical and organisational measures (e.g pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

We shall assess what privacy by design measures can be implemented on all programs / systems / processes that process personal data by taking into account the following:

- The cost of implementation
- The nature, scope, context and purposes of processing
- The risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

DPIAs must also be conducted in relation to high risk processing.

We shall conduct a DPIA and discuss our findings with the Operations Manager when implementing major system or business change programs involving the processing of personal data including:

- Use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes)
- Automated processing including profiling
- Large scale processing of special category data
- Large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- A description of the processing, its purposes and the data controller's legitimate interests if appropriate
- An assessment of the necessity and proportionality of the processing in relation to its purpose
- An assessment of the risk to individuals
- The risk mitigation measures in place and demonstration of compliance.

We shall inform the Operations Manager at the initial stage of any new project.
Please see appendix B for a DPIA assessment template.

Direct Marketing

We are subject to certain rules and privacy laws when marketing to the members of congregation.

For example, a data subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing members of congregation known as "soft opt in" allows Trinity Cheltenham to send marketing texts or emails if they have obtained contact details in the course of a service to that individual, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject's objection to direct marketing must be promptly honoured. If a member of congregation opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

Automated Processing and Automated Decision Making

We do not conduct any automated decision making.

Changes To This Data Governance Policy

We reserve the right to change this Data Governance Policy at any time without notice to you so please check back regularly to obtain the latest copy of this policy. We last revised this Privacy Standard in June 2020

Appendix A- Record Retention Schedule

Human Resources	
Personnel and training records (including disciplinary and grievance hearing notes)	6 years after employment ceases
Appraisals records	5 years
Sickness Records	3 years after year ends
Employee Treatment records	6 years
Details of medical schemes	Permanently
Life assurance expression of wish forms	6 years after employment ends / after death
Statutory maternity pay records, calculations,Certificates or other medical evidence	4 years
Pensions scheme - next of kin / expression of wish form	6 years after death
All trust deeds, rules & minute handbook Annual records & Inland revenue contribution records	Permanent
Pension scheme investment policies	12 years after paid benefits stop

Payment records	6 years after payment
Group health policies	12 years after benefit ceases
Wage / salary records (also overtime, bonuses, expenses)	6 years
Application forms and interview notes (for unsuccessful candidates)	6 months to a year. (Because of the time limits in the various discrimination Acts, for example the the Disability Discrimination Act 1995, minimum retention periods for records relating to advertising of vacancies and job applications should be at least 6 months. A year may be more advisable as the time limits for bringing claims can be extended. Successful job applicants documents will be transferred to the HR file in any event).
Parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
HR files and training records (including disciplinary records and working time records)	6 years after employment ceases
Senior employees records	Permanently for historical purposes
Job adverts	1 year
Health and safety records	3 years
Complaints	
Complaint enquiries and correspondence	6 years
Register of complaints	6 years
Compliance	

Whistleblowing records	6 years
Gifts and Hospitality Register	3 years
Records relating to serious matters of: • theft • fraud • misappropriation • recoverable debts and overpayments • write-offs • recovery of debt • wavering of debt (where external action has been taken)	10 years after action/investigation is completed
Records relating to minor matters of: • theft • fraud • misappropriation • irrecoverable debts and • overpayments • write-offs • recovery of debt • wavering of debt (where matter was resolved internally)	10 years after action/investigation is completed
SAR requests	6 years
Risk assessments	6 years
Breach reports	6 years
Adhoc	
Meeting minutes	5 years
Leadership and Committee papers	Life of the organisation
Leadership and Committee agendas	Life of the organisation
Leadership and Committee minutes	Life of the organisation

Insurance	
Employers' liability	Permanently
Public Liability	Permanently
Professional indemnity	Permanently

Appendix B- Data Protection Impact Assessment

1. Administrative information

Stakeholders and contact details
Name of Initiative: [Initiative/Initiative name]
Name and role of organisation completing the DPIA: [Organisation name Controller/Processor]
Functional area responsible for the Initiative: [For example, Technology, HR, Finance, Alliances, Procurement.]
Initiative project manager: Name: Email Address: Mobile Phone/Direct Dial:
Other stakeholders: Name: Email address: Mobile phone/direct dial:
Third parties involved/associated with the Initiative [These are as listed in Section 10]
Relevant documents

[Identify relevant documents and consider including copies as an Annex.] [Initiative/Initiative business case]] [Design documents] [Previous DPIAs] [DPIAs covering related processing operations] [Documents to refer to: Privacy policy, Relevant legislation, DPA Guidance, ICO Guidance, European Data Protection Board Guidelines, Codes of Conduct, Other policies: [for example, Information security, Data retention, HR, Marketing, Finance].]

2. Overview

How to read the DPIA: [Living document]
High level description of the Initiative: [In this section include a high level description of the Initiative, so that it is easy to then explain the scope of the DPIA in the context of the overall initiative.]
Relationship between the DPIA and the Initiative: [Explain the scope of the DPIA in the context of the overall initiative.]
Context: [Consider: Pilot Pha se Initiative vs Programme Related processing activities]
Key parameters (for example, boundaries of DPIA). What is in scope and excluded from scope?: [It may be useful to describe the boundary lines of the DPIA and what is covered by the assessment. Note that this may be different to the boundary of the Initiative.]
Rationale as to why a DPIA is required: [Processing is high risk, [explain why].]
Multiple sets of data processing operations: [If the DPIA covers multiple sets of data processing operations provide further explanation here.]

3. Consultation

Advice of person responsible for data:
Input of specific business functions: [Record the advice/input of specific business functions that are stakeholders/have an interest in the Initiative.]

Input of data subjects and/or their representatives:
[- Explain how the views were sought. For example, obtained through studies, questionnaires, discussion with data subject representatives (customers, staff, Works Council).
- Final decision - if different from Data subject's views to include rationale for proceeding
- Justification for not seeking input from Data subjects for example, compromises confidentiality of business plans, disproportionate, impractical.]

Input of experts and other interested stakeholders:
[Record the advice/input of independent experts of different professions (such as lawyers, IT experts, security experts, sociologists, ethics experts) as well as other stakeholders who have an interest in the Initiative.]

4. Scope

Description:
[High level description of Initiative including technical capabilities/ functionality Assets/technology involved with processing the personal data:

a. Hardware
b. Software
c. Networks
d. People
e. Paper
f. Paper Transmission Channel(s)
g. Mobile Devices
h. Cookies
i. Other such as cloud, data warehouses etc.

Business context:
[It is often useful to explain the background/business context to the Initiative. This will also help when discussing the objectives and benefits of the processing.]

Types of data subject:
[For example, children, student, consumer, customer.]

Initiative's objectives and scope:
[To be confirmed – this section may be merged with Business context above.]
Boundaries - in scope and out of scope:
[In this section you are considering the boundaries of the Initiative, not the boundaries of the DPIA.]

5. Description of processing

Data flow map(s):
Data entry and exit points, location, user categories, data subject categories

Description of the proposed processing operations:
[To be confirmed – this section may be merged with Description in the Scope section, Section 5 above]

Types of personal data:
[Identification of categories/types of personal data collected]
Types of data subject: [Identification of categories/types of data subject.]
Sources of the personal data: [- Feeds from systems (internal/external) - Purchased lists - Collected directly from data subjects]
Length and frequency of processing:
Processing volumes: [Volumes - Data subjects and records Volumes of certain types of data subject (such as children; vulnerable individuals) Volumes - users and type Type of users - internal, external (such as affiliates, vendors and alliance partners)]
Data minimisation: [Identify considerations given to data minimisation (such as certain types of data subject not included in scope, types of data/fields collected minimised, data flows minimised, de-identification techniques used).]

6. Basis of processing

Lawful processing
Necessity and proportionality assessment (assessment of the necessity and proportionality of the processing operations in relation to the Purpose(s)): [Purpose limitation: • Specified, explicit and legitimate purposes(s) Lawfulness of processing • Grounds • Consent • Legitimate interest *1.* Balancing test – assess whether legitimate interests are overridden by the interests or fundamental rights and freedoms of the data subjects *2.* Adequate, relevant and limited to what is necessary *3.* Limited storage duration • Measures contributing to the rights of the data subjects]
Rights and freedoms assessment (assessment of the risks to the rights and freedoms of the data subjects):
Fair processing

Business continuity:
System decommissioning: [Identify any systems which need decommissioning. Consider associated issues such as data migration and secure data deletion.]

Fair processing: [Fair processing requirements: *1.* Information provided to the data subject (privacy notice) *2.* Use of cookies]

7. Purpose(s) of processing; benefits and risks

Purpose(s) of processing
[Automated processing (including profiling) Evaluation or scoring (including profiling or predicting) Automated decision making with legal (or similar) effect
Large scale processing of data Sensitive data or data of a highly personal nature Systemic monitoring of publicly accessible area Creation or use of personal profiles Matching/ combining datasets Vulnerable data subjects Innovative use or applying new technologies or innovative solutions Processing in itself "prevents data subjects from exercising a right or using a service or a contract Other [marketing, analytics]]
Benefits
[Individual(s) [Data subjects, users] Group of individuals Organisation(s) [Data controller, third parties] Society]
Risks
[Types of risk Possible threats/sources of risk Likelihood of risk occurring Impact if risk occurs/type of damage Risk mitigation options]

8. Countries

Country summary: [Provide an overview of all the countries that the personal data touches]
Location of data subjects:
Location of users: [Consider: Employees Contractors Third Parties]
Hosting location:
Support and maintenance: [Consider application support and maintenance but also customer support]
Country specific documents: [See Annex e.g. Local language privacy notices]
International data transfer arrangements:
Name and role of parties receiving the personal data:
Grounds for transfer: [Binding Corporate Rules EU Model Clauses Privacy Shield]

9. Disclosure to third parties

Recipients: Name: Address: Role: Data to be disclosed: Role of the recipient:
Reasons for disclosure Agreements Need for separate DPIAs Monitoring arrangements/contract management

10. Security of processing

Practical safeguards: [Examples: Identity and access management arrangements Examples: Training, communication and awareness Examples: Due diligence arrangements re: third parties Examples: Contract management and monitoring arrangements with third parties] Security measures: [Examples: Encryption Examples: Arrangements re: data security breach notification] Mechanisms to protect personal data: [Examples: De-identification of data Examples: Arrangements re destruction of data Examples: Data back-up/disaster recovery arrangements] Mechanisms to demonstrate compliance with legislation: [Examples: Maintenance of records such as re: consents, privacy notices, data flow maps, approvals.]

11. Data quality

Assessment of quality: [Checking that data sets are comprehensive, complete, without bias, accurate. Balancing with the need for data minimisation.]
Review arrangements: [Arrangements to review the data sets and to keep information up to date and accurate.]

12. Arrangements to address individual rights

Right to be informed:
Right of access:
Right to rectification:
Right to erasure/right to be forgotten:
Right to object and restrict processing:
Right to data portability:
Rights in relation to international transfer(s):
Rights in relation to prior consultation:
Rights in relation to automated decision-making and profiling:

13. Retention and disposal

Retention periods: [Identify how long the different types of data will be stored for.]
Archiving:
Back-up:

14. Special arrangements for vulnerable individuals

Category of vulnerable individuals: [Look for instances of imbalance of power between the data controller and data subject and identify types of individuals involved where this exists.]
Special arrangements required: [What arrangements, if any, are required? Examples might be special arrangements for consent, or adjustments to privacy notices.]

15. Actions

Action required	Owner	Date to be completed

16. Decision

Decision: [Proceed with Initiative/Not proceed with Initiative]
Authorised person: Date: