

Data Protection Policy



Document Control	
Approved by:	MannionDaniels Senior Leadership Team
Responsible Owner:	Operations Team
Created:	04 April2016
Revised:	04 February 2020
Approved:	05 February 2020
Next Review:	04 February 2021
Version:	4

Table of contents

1	Introduction	4
1.1.	Scope of Policy	4
2	Policy Statement.....	4
3	General Principles	4
4	Data Protection Roles and Responsibilities	5
4.1.	Data Controller	6
4.1.1	Data Protection Officer (DPO)	6
4.2	Senior Leadership team - Information Security responsibilities	6
4.2.1	Information Security Officer	6
4.3	Senior Management Team - Information Security responsibilities	6
4.4	All Employees/Staff	6
4.5	Consultants, Suppliers and Others	7
5	Data Protection additional definitions.....	7
5.1	Information Commissioner's Office	7
5.2	Data Subject	7
5.3	Data Processor	7
5.4	Data Processing	7
5.5	Data User	8
5.6	Data Recipient	8
5.7	Personal Data Third party	8
6	Type of Information Processed	8
6.1.	Non-exhaustive list of personal information processed by MannionDaniels ...	8
6.2	Forms of personal information	9
6.3	Processors of personal information	9
6.4	Personal data flow diagrams	9
6.5	Exemptions	9
7	Data Collection and Rights of Access	10
7.1	Transferring Data	10
7.2	Sharing Data	10

7.3 Data Subject Access Request (SAR)	10
7.4 Freedom of Information Act	10
8 Data Management	11
8.1. Data Management principles	11
8.2 Storage and handling data records	11
8.3 Data access	11
8.4 Tracking data records	11
8.5 Data Suspension	11
8.6 Data Retention and Data Disposal	12
8.6.1 Principles of data retention (management) and data disposal	12
8.6.2 Protocol of data retention (management) and data disposal	12
8.6.3 Data disposal methods	12
8.7 Training	13
8.8 Complaints	13
9 Data Protection Breaches.....	13
9.1. Breach Incident Procedure	13
9.1.1 Data breach reporting and containment phase	13
9.1.2 Breach Response phase	14
9.1.3 Breach Recording	14
9.2 Breach Notification	14
9.2.1 Supervisory Authority Notification	15
9.3 Record Keeping of Data Breach records	15
10 Annexes.....	15
10.1 Annex 1 Exemptions	15
10.2 Annex 2 European Economic Area (EEA)	15
10.3 Annex 3 Data Breach Procedure	17
10.4 Annex 4 Data Breach Incident Form	18
10.5 Annex 5 Disposal/retention criteria checklist	20
10.6 Annex 6 Retention Guidelines	22
10.7 Annex 7 Possible data breach responses	26

Picture credits

Cover, left and on table of contents,
left: Team Kenya
Cover, right: Send a Cow

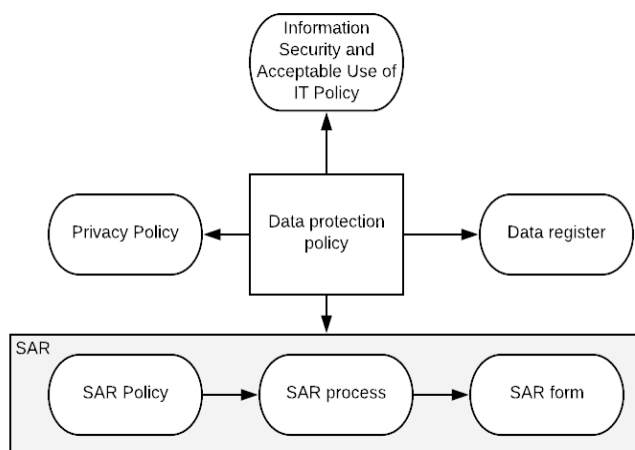
1 Introduction

MannionDaniels needs to keep certain information about its employees, clients, donors and other stakeholders to enable us to deliver services. It is also necessary to process information, so employees can be recruited and paid, projects delivered and legal obligations to funding bodies, government and third-party partners met. MannionDaniels recognises the importance of preserving privacy and protecting personal data and is committed to complying with the principles of the Data Protection Act 2018 (DPA18) and the EU General Data Protection Regulation (GDPR).

1.1 Scope of Policy

This policy applies to all employees on a permanent or fixed term contract and to all associated individuals, contractors, third party representatives etc, engaged by the company in the UK or overseas and for any MannionDaniels subsidiary companies. All contractors and agents acting for and on behalf of the company should be made aware of this policy. This policy applies to all personal and sensitive personal data processed on computers and stored in manual (paper-based) files.

This policy while mentions some of the aspect of Information Security, Privacy policy and right of access, does not cover mentioned areas in depth. Following diagram offers graphical representation of relationships between Data Protection Policy and related documents.



2 Policy Statement

MannionDaniels regards the lawful and correct treatment of personal information as very important to successful operations and to maintaining the confidence of all our stakeholders. We will do everything within our authority to demonstrate our commitment and endorsement of the Principles of the DPA18 and GDPR, and ensure the organisation treats personal data and the rights of individuals with respect.

To this end, we fully endorse and adhere to the Principles of Data Protection as enumerated in the DPA18 and GDPR, and we commit to:

- Comply with both law and good practice
- Respect Individual's rights
- Be open and honest with individuals whose data is held
- Provide training and support for staff who handle personal data, so they can act confidently and consistently
- Notify the Information Commissioner's Office (ICO)

To meet our responsibilities all staff and individuals who process data on behalf of MannionDaniels will:

- Ensure any personal data is collected in a fair, transparent and lawful way;
- Explain why the data is needed at the start of the point of collection;
- Ensure that only the minimum amount of information needed is collected and used;
- Ensure the information used is up to date and accurate;
- Review the length of time information is held;
- Ensure the rights people have in relation to their personal data can be exercised

3 General Principles

The GDPR sets out seven key principles which MannionDaniels comply with:

- Lawful, fair and transparent processing – When the data is collected, it must be clear as to why that data is being collected and how the data will be used.
- Purpose limitation – There must be a lawful and legitimate purpose for processing the information.
- Data minimization – Data captured must be adequate, relevant and limited.
- Accurate and up-to-date processing – Ensure information remains accurate, valid and fit for purpose.
- Limitation of storage in the form that permits identification – Discourage unnecessary data redundancy and replication and controls storage and movement of data.
- Confidential and secure – Protect the integrity and privacy of data by making sure it is secure (which extends to IT systems, paper records and physical security).
- Accountability and liability – Demonstrating compliance by ensuring every step within the GDPR strategy is auditable and can be compiled as evidence quickly and efficiently.

There are strict procedures on how we comply with the GDPR. All data users must follow MannionDaniels procedures to ensure MannionDaniels complies with the fair and lawful processing of personal data. See the Data Protection Procedure and Guidelines for more detail.

Non-Compliance

The aim of this policy is to embed the principles of data protection across the breadth of our business interests and protect all those with whom we have a relationship with. Data privacy is relevant to and the responsibility of everyone.

The DPA is enforced in the UK by the Information Commissioner's Office (ICO). The ICO has a number of powers including the ability to fine organisations up to €20 Million or 4% of the global annual turnover and publicise information about data protection breaches. They can also prosecute those who commit criminal offences under the Act

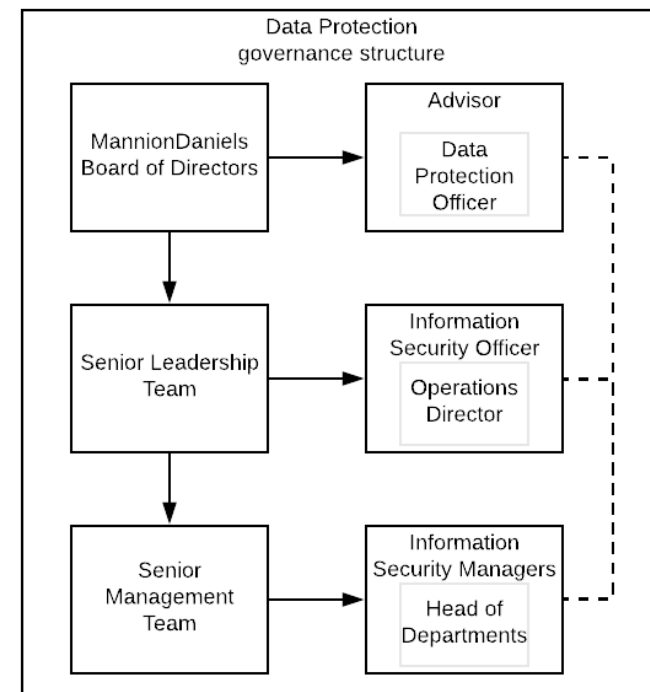
Data protection breaches may be conducted wilfully, negligently or unintentionally. Any data breach or failure to follow this policy is likely to result in disciplinary procedures being applied.

Suppliers and subsidiaries of MannionDaniels

As a matter of good practice, other agencies and individuals working with MannionDaniels, who have access to personal information, will be expected to have read and to comply with this policy. It is expected that individuals in the organisation who deal with external agencies or partners will take responsibility for ensuring an appropriate contract is in place to ensure compliance with this policy and related requirements under the GDPR.

4 Data Protection Roles and Responsibilities

For the purposes of the GDPR, MannionDaniels is the "data controller". We are wholly committed to ensuring the Company adheres to its responsibilities and have identified the governance structure below:



4.1 Data Controller

MannionDaniels Board of Directors is accountable and has overall responsibility for the company's compliance with data protection and determines the purposes for which and the way personal data are to be processed.

4.1.1 Data Protection Officer (DPO)

The Board of Directors appointed Data Protection Officer at the capacity of an advisor in the data protection related matters.

The Data Protection Officer has the following responsibilities:

- Briefing the Board/Leadership Team on Data Protection responsibilities and issues
- Advising other staff on difficult Data Protection issues

4.2 Senior Leadership Team – Information Security responsibilities

Senior Leadership Team has overall responsibility for information security in all parts of MannionDaniels' business areas. The Senior Leadership team has appointed Operations Director as an Information Security Officer to oversee all elements of data protection implementation and report back to the Leadership Team.

4.2.1 Information Security Officer

Director of Operations has been appointed as the Information Security Officer who has a day to day responsibility for ensuring Data Protection Policy is implemented and adhered to. Operations Director is also the point of contact with our IT providers to ensure security is maintained and updated in accordance with new technological developments.

Responsibilities of Information security Officer: Data Protection Officer has the following responsibilities:

- Reviewing Data Protection and related policies, implementing and enforcing
- Ensuring regular checks are undertaken by managers and supervisors
- Identifying and addressing areas where there is a risk of a data protection breach
- Ensuring that Data Protection induction and refresher training takes place
- Representing and corresponding with the Information Commissioner's Office (ICO) maintaining the accuracy and currency of the organisation's notification
- Handling Subject Access Requests
- Approving contracts with Data Processors
- Approving unusual or controversial disclosures of personal data
- Undertaking internal audits and ensuring appropriate records are maintained to demonstrate compliance and reporting to Board/Leadership Team

4.3 Senior Management Team – Data management responsibilities

The Senior Management team has a responsibility for hands-on implementation of the data protection and information security principles within the departments of MannionDaniels. Head of Departments and Contract leads are acting as a Information Security Managers in their department/contract.

Each head of the department/ contract lead is responsible for:

- Ensuring staff are aware of and abide by this policy, associated guidance and for identifying needs for additional training.
- Ensuring all staff are responsible for the security of information within their area and applying good information handling practice within the organisation.
- Directing any concerns or queries to DPO or Information Security Officer.

4.4 All Employees/Staff

All staff who collect, process or manage information about other staff or third parties must comply with this policy and related guidance. Staff must ensure

personal data is kept securely and is not disclosed to any unauthorised third party. Diligence should be applied to confidentiality requirements, particularly when determining whether the information is appropriate to disclose, and extreme care should be taken to ensure the safety of personal data. (Please see guidance for staff).

All staff are responsible for checking any information provided to MannionDaniels about their employment is accurate and up-to-date. They should contact the HR Manager to inform them of any changes to personal information provided, such as a change of address, or whether the information we hold has errors or is inaccurate. All employees who hold or process personal data are considered to be "Data Users".

4.5 Consultants, Suppliers and Others

MannionDaniels engages suppliers who may be contractors, independent consultants, temporary workers, associates and interns. All those who undertake work on behalf of MannionDaniels are considered to be "Data Users" and must comply with this policy and understand their obligations and responsibilities to ensure compliance with Data Protection.

Provision will be made in contracts with external providers and consultants to ensure compliance with this Data Protection Policy and the GDPR. Where third parties undertake work on behalf of MannionDaniels we remain the data controller and must take appropriate measures to ensure the contract is explicit on third party obligations.

5 Data Protection additional definitions

5.1 Information Commissioner's Office

The ICO (Information Commissioner's Office) is the regulatory body which oversees compliance with the Act. It:

- Sets guidance for organisations to help them and their staff comply with the Act;
- Provides advice to organisations on how to comply with the Act;

- Investigates complaints made by individuals who believe there has been a breach;
- Has power to take action against organisations who do not comply, or where there has been a breach, including enforcement notices, monetary fines and criminal sanctions.

5.2 Data Subject

A person or individual who is the subject of personal data. Within the workplace, they may be current employees, people applying for jobs or former employees. Data subjects might also be customers, suppliers, clients or other people about whom information is held. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

5.3 Data Processor

Means any person (other than an employee), who processes data on our behalf. Data Processors must also ensure they follow the principles of the act and make sure information is handled correctly; data processors will include organisations processing payroll, IT providers or other services outsourced by the organisation.

5.4 Data Processing

The term processing refers to a wide range of actions relating to personal data which includes obtaining, holding, recording, consultation or retrieving the data, or doing work on the data such as organising, adapting, changing, disclosing, erasing or destroying it. Any activity or operation carried out in relation to data is likely to fall within the definition of processing. MannionDaniels also use external organisations to process data on our behalf (IT, payroll etc) and these organisations are classed as Data Processors. Note MannionDaniels maintain responsibility for any breaches made by data processors.

5.5 Data User

All staff and other individuals who process data on behalf of MannionDaniels are a data user. Where your role requires you to process personal data your area data user and must comply with all the data protection principles

5.6 Data Recipient

Any person to whom the data are disclosed including any employee or agent of the data processor. The data controller's notification to ICO must include any description of any "recipient or recipients to whom the data controller intends or may wish to disclose the data".

5.7 Personal Data Third party

In relation to personal data, means any other person other than

- the data subject,
- the data controller, or
- any data processor or
- other person authorised to process data for the data controller or processor.

6 Type of Information Processed

MannionDaniels collects personal data in many ways including application forms, CVs, letters, emails, appraisals, payroll information, et.al. The data is processed as part of our everyday operations. In all cases, there should be valid and explicit reasons for collecting personal data, for holding and processing and for how long it is held

The data is collected and used for many purposes, of which these are the main categories:

- Obligations under the employment contract, (recruitment, training, appraisal, remuneration, welfare etc);

- Legitimate business purposes, (career planning, financial monitoring and decision-making, administration and security arrangements etc);
- Legal and regulatory requirements; and
- Provision of service through our contracts with third parties and partners

6.1 List of personal information processed by MannionDaniels

MannionDaniels processes the following personal information.

Personal Details:

- Name
- Postal address
- Email address
- Skype address
- Phone number
- Emergency contact, next of kin information
- Nationality
- Gender
- Date of birth
- National Insurance number
- CV
- Passport, copy of a passport
- Short biography
- Cover letter

Personal financial information:

- Bank details (account number, sort code, bank addresses)
- Salary information, daily rates of consultants
- Organisational financial records such as annual accounts
- Salary related transaction information
- Payment information

Previous and current employment related information:

- Job role information; job title
- Name of organisation
- Previous employment details; references
- Employment performance information; working hours, work absences
- Financial claim details

- Employment start and end date
- Employee pension contribution
- Travel information

Sensitive medical information:

- Medical information
- Medical conditions
- Health issues and medication
- Blood group

6.2 Forms of personal information

Personal information is kept in the following forms:

- Databases and electronic formats
- Manual paper records

6.3 Processors of personal information

Groups of people within the organisation who will process personal information are:

- Directors
- Senior Managers
- Project Managers and Project Officers
- HR and Office Managers
- Technical Leads and Specialists
- Fiduciary Risk and Finance Teams
- Communications Team
- Consultants of MannionDaniels
- Suppliers of MannionDaniels

If an individual does not consent to certain types of processing (i.e. DBS checks as part of integrity due diligence), appropriate action must be taken to ensure that the processing does not take place.

Personal data register document includes exhaustive list of following information:

- The list of collected personal data types
- The list of retention periods for each type of collected personal data
- The list of purposes for collection of each type of personal data
- The list of systems used for processing and storage of personal data including their security measures
- The list of teams with the access to the personal data
- The list of external partners with the access to the personal data

If any member of staff or associate is in any doubt about these matters, they should speak to their manager, Operations Director or contact the Data Protection Officer to seek clarification BEFORE taking any action.

6.4 Personal data flow diagrams

The personal data flow maps include following departments and areas.

Departments	List of related processes
Human resources	- Recruitment process - HR processing
Finance	- Finance and Accounting
Communications	- Communication processing
PFM&FR	- Due diligence process - Financial audit of grantees process - Fiduciary processing of UK Aid Match appeals - Financial claims approval process
Operations	- Procurement process - Travel management process - Business development process

Grant making contracts/projects	List of Related processes	
Amplify Change	- Amplify Change grant management process	Grant application process

UK Aid Direct	- UK Aid Direct grant management process	
UK Aid Match	- UK Aid Match grant management process	

The personal data flow diagrams together with the manual how to read personal data diagrams can be found in Annex 8.

6.5 Exemptions

MannionDaniels' approach is to assume that all personal information collected and processed is subject to the Data Protection Act. However, in certain circumstances, particularly where this involves some public interest, data may be disclosed to third parties. The majority of these exemptions only allow disclosure and processing of personal and sensitive personal data where specific conditions are met. Please see Annex 1 for more detailed information on exemptions.

7 Data Collection and Rights of Access

Where MannionDaniels collects personal data, the MannionDaniels Privacy Notice will be available to the data subject at the time of collection, or as soon as practicable after. This will be a link to the web page or in hard copy.

Where MannionDaniels engages third party organisations to process data on their behalf, we will ensure all contracts with data processors contain model contracts to ensure data processors comply with our instructions and obligations under the GDPR. We will ensure we choose data processors who provide sufficient guarantees in respect of security measures and they comply with obligations equivalent to those imposed on MannionDaniels as Data Controller.

7.1 Transferring Data

Information that we collect may be stored and processed in and transferred between any of the countries in which we operate. MannionDaniels in our normal course of business will undertake transfer of data to countries outside of the European Economic Area (EEA). This is inherent, known and necessary in the work we do, and in our organisational structure.

Our clients, partners and other stakeholders are often located in countries outside of the EEA. As such MannionDaniels take steps to ensure that we comply with all the principles of the DPA and this policy and related policies when transferring data. See Annex 2 for a list of countries in the EEA area.

7.2 Sharing Data

MannionDaniels shares personal data within the organisation and with external organisations to achieve our obligations under the employment contract and contracts relating to our core business. Where sharing information internally it is the responsibility of the requesting and receiving member of staff to ensure they have authority to access/disclose the information. If in doubt advice should be sought from the Information Security Officer or Data Protection Officer.

When sharing personal data externally we must comply with the GDPR and ensure we comply with our duty to treat individuals fairly. Before sharing personal data, all staff must check with the senior manager. If the senior manager is not certain that the sharing of personal data is compliant with GDPR then Operations Director is contacted. If Operations Director is not certain, DPO is contacted to advise. The personal data should not be shared unless there is highest level of certainty that the sharing is compliant with GDPR, which means there is a clear legitimate reason why the information should be shared, and all eight data protection principles are adhered to.

7.3 Data Subject Access Request (SAR)

Please refer to MannionDaniels Subject Access Request Procedure document.

7.4 Exemptions

The Freedom of Information (FOI) Act 2000 came into effect on 01 January 2005. It aims to promote a culture of openness in the public sector by giving access to all recorded information held by it (subject to exemptions). The Freedom of Information Act does not currently apply specifically to private organisations. However, as MannionDaniels provides contractual services to Government Bodies it may be deemed that we are holding information on behalf of a public body. Where such public body receives a FoIA request this may result in MannionDaniels being required to disclose confidential information and intellectual property.

The FOI may affect MannionDaniels indirectly and it is important that staff are aware the organisation may be subject to disclose information. Any requests received should be directed to your line manager in the first instance who will liaise with the Data Protection Officer and appropriate Director(s).

For additional information how MannionDaniels approaches Information Security, Privacy policy and right of access, please refer to the following related policies and procedures:

- Information Security and Acceptable Use of IT Policy
- Privacy Policy
- Subject Access Request Procedure

8 Data Management

It is necessary to abide data protection management practices which will help us to deliver and meet our statutory duties and support our aim to be a highly respected organisation. Abiding with the Data Protection management practices MannionDaniels aim to ensure that the data, whatever form it takes, is accurate, reliable, ordered, complete, useful, up-to-date and accessible whenever it is needed to help us perform at the optimum level. MannionDaniels have in place detailed procedures for the Data Management. Key procedures are defined in this policy or other MannionDaniels policy documents. The policy documents to be referred to include:

- Data Protection Procedure and Guidelines
- Information Security and Acceptable Use of IT Policy

8.1 Data Management principles

As soon as a data is created or received during the course of MannionDaniels business an appropriate record keeping system should be implemented. All data records should be available and accessible with the appropriate access level for the requirements of business operations.

All record systems should be designed to ensure the integrity, accuracy and safe storage of the data in question. This will aid smooth transfer when a system application is being replaced or superseded and protect the data from being lost or misplaced. Data should be retained in line with the Data Retention and Data disposal principles (see section 8.6.1), Data Retention and Data disposal protocol (see section 8.6.2) by using appropriate Data disposal method (see section 8.6.3).

8.2 Storage and handling data records

All data should be stored on media that ensures their security, integrity, reliability, usability and authenticity and in a way that takes account of the records' specific physical properties. Storage conditions and handling processes should ensure the records are protected from unauthorised access, loss or destruction and from theft. For more guidance on data management in digital form, please, refer to MannionDaniels Information Security and Acceptable Use of IT Policy.

8.3 Data access

Access to records should be governed in a way that reflects business needs and requirements and ensure there is no opportunity for the records to be disclosed, deleted, altered or destroyed, either accidentally or intentionally.

8.4 Tracking data records

It is imperative that the systems put in place allow retrieval, monitoring, appropriate disposal of data when they are no longer needed and comply with security practices. Any modifications or alterations to data records should be

monitored and an audit trail demonstrating the historical involvement of the data records. MannionDaniels has a data register which serve to track and monitor data used and processed by MannionDaniels. It is a responsibility of all members of Senior Management Team to keep the data register up to date.

8.5 Data Suspension

The data should be immediately suspended in the event of litigation, claim or dispute where MannionDaniels is involved. The suspension of data means preserving information potentially relevant to litigation, investigations or other disputes, as well as any steps MannionDaniels must take to ensure that data maintains its evidentiary integrity.

8.6 Data Retention

The purpose of this Data Retention and Data disposal section is to provide an organisation-wide framework to govern management decisions on whether a particular data (or set of data in the records, including electronic versions) should either be:

Retained –and if so in what format and for what period; or

Disposed of –and so when and by what method

8.6.1 Principles of data retention (management) and data disposal

The underlying principle of data management and disposal is to ensure that a data is managed through its life cycle from creation or receipt, through maintenance and use to disposal.

Good data management relies on the following:

- Understanding what data needs to be captured and stored
- Understand how long we need to retain data
- Understand data tracking mechanisms; and data disposal at the right time

Each department must understand data retention requirements for data within their department. The Data Protection Policy offer disposal/retention criteria as a default position the retention period might be longer as a result of the

contractual requirements. If the disposal / retention criteria differ from contractual requirements, it is important the longer retention period is always respected.

All data retention periods must be recorded in the data register.

8.6.2 Protocol of data retention (management) and data disposal

Any decision whether to retain or dispose of a data should be taken in accordance with the retention/disposal protocol. This protocol consists of following steps:

- Step 1 – Check against key disposal/retention criteria
No data should be disposed before the key disposal/retention criteria have been considered in relation to data. Please, find the key disposal/retention criteria checklist in Annex 5.
- Step 2 – Check against retention schedule
The Retention Guideline (see in Annex 6) provide guidance on recommended and mandatory minimum retention periods for specific classes of data/records/documents.

Where a retention period has expired in relation to a particular data a review should always be carried out before a final decision is made to dispose of that data. Such reviews need not necessarily be detailed or time consuming.

In the event that a decision is taken to dispose of a particular document or set of documents, then consideration should be given to the method of disposal and a log made when the record is disposed.

8.6.3 Data disposal methods

Once records have been retained for the applicable period they should be prepared for disposal;

- Paper record should be shredded.
- Electronic data should be deleted permanently (including the bins) not available for retrieval.

- Electronic data contained on servers and hard drives should be deleted and overwritten.
- Electronic data contained on all other media should be destroyed by the physical destruction of that media.

As guidance however, staff should take into account the following considerations when selecting any method of disposal:

- Under no circumstances should paper documents or removable media (CDs, DVDs, discs, etc) containing personal data or confidential information be simply binned or deposited in refuse tips. To do so could result in the unauthorised disclosure of such information to third parties and render MannionDaniels liable to action under the Data Protection Act. Such documents should be destroyed on site (e.g. by shredding) or placed in "Confidential Waste" refuse bins.
- Deletion –the Information Commissioner's Office has advised that if steps are taken to make data virtually impossible to retrieve, then this will be regarded as equivalent to deletion.
- Recycling –wherever practicable disposal should further recycling, in-line with MannionDaniels 'commitment to the environment.

8.7 Training

Training on Data Protection is mandatory for all employees. All new employees will receive training on this policy and the related policies and procedures referred to above.

Refresher training will be conducted on a regular basis for existing employees and managers should include data protection on their agendas for team meetings; this will ensure we are reinforcing our desire to respect the information of data subjects and promote best practice and consistent standards

8.8 Complaints

If anyone is dissatisfied with the way in which we have handled your personal data, please contact the Data Protection Officer. We take very seriously our responsibility under the Data Protection Act and consistently strive to

collaborate and improve our standards.

If, after this, you are still dissatisfied with how MannionDaniels have managed your data, you also have the right to lodge a complaint with the Information Commissioner's Office. You can find details about how to do this on the ICO website at <https://ico.org.uk/concerns/> or by calling their helpline on 0303 123 1113.

9 Data Protection Breaches

MannionDaniels has robust objectives and controls in place for preventing data breaches and for managing them in the rare event that they do occur. We have developed a structured and documented breach incident program to mitigate the impact of any data breaches and to ensure that the correct notifications are made. Any member of the team dealing with data breach is encouraged to communicate with Data Protection Officer.

The breach incident procedure consists of two phases:

- Data breach reporting and containment phase; and
- Data breach response phase

9.1 Breach Incident Procedure

Reporting incidents fully and with immediate effect is essential to the compliant functioning of the MannionDaniels and is not about apportioning blame. These procedures are for the protection of the Company, its staff, customers, clients and third parties and are of the utmost importance for legal regulatory compliance.

9.1.1 Data breach reporting and containment phase:

1. Data breach is identified
2. Person who identifies the data breach notifies operations team on operations@manniondaniels.com
3. Project operations team sends data breach form section 1 (please see annex 4) to be filled by the person who notified about the data breach
4. Notifier fills the data breach form section 1 and send it back to the

project operations team to operations@manniondaniels.com

5. After receipt of the breach form filled by notifier project operations team check all required information about data breach are filled in the breach form section 1 (please see annex 4) and notify Operations director and Head of operations
6. Operations Director and Head of operations will perform data breach review which consist of
 - a) Identification of a root cause of a data breach
 - b) Identification of a scale of data breach (if IT department is impacted by the data breach then data breach form section 3 needs to be filled by IT department)
 - c) Agreement of a containment of a data breach
 - d) Assessment of the risk level of a data breach
 - e) Notification of Data subject (if necessary)
 - f) Notification of ICO (if necessary)
 - g) Appointment of a team leader for the data breach

All the decisions and findings of data breach review are recorded in the data breach form section 2 (please see annex 4).

9.1.2 Data breach response phase:

7. Data breach team leader appoints data breach team
8. Data breach team performs
 - a) full risk analysis and gap analysis;
 - b) proposes mitigation action plan
 - c) notifies Senior Management team about the proposed mitigation action plan
9. Senior Management team assess the proposed mitigation action plan and approves it
10. Operations director oversees the implementation of the approved mitigation action plan

All the decisions and findings of data breach response phase are recorded

in the data breach form section 4 (please see annex 4).

9.1.3 Breach response phase:

If the information from Data breach form Section 1 indicate that the breach is a result of a cyber incident or system error, then IT Department will be immediately notified to fill the data breach form Section 3 and will be actively involved in identification of a most appropriate mitigation plan. Once the Section 3 of a data breach form is filled it will be reported to Operations Director.

The breach response phase objectives are to provide gap analyses and risk analyses of data breach. Operations team is leading this phase by filling the data breach form Section 4. Operations Director is responsible all elements of breach response phase such as risk assessment, gap analysis, root cause analysis, et. al. is accomplished.

Once, the analyses are finalised Operations team will identify the most appropriate response to data breach in the form of a mitigation plan. The operations team will suggest the person who will be responsible for implementation of the selected mitigation plan after it is approved by the Leadership team.

Some of the possible breach responses are listed in Annex 7.

9.1.4 Breach Recording

MannionDaniels utilises a Breach Incident Form (see Annex 4) for all incidents, which is completed for any data breach, regardless of severity or outcome. Completed forms are logged in the Breach Incident log and reviewed against existing records to ascertain patterns or reoccurrences. All documents related to the Breach incidents are filed in the Breach Incident folder.

If applicable, the Supervisory Authority and the data subject(s) are notified in accordance with the GDPR requirements (refer to Breach notifications section of this policy). The Supervisory Authority protocols are to be followed and MannionDaniels Data Breach Form should be completed and submitted. In addition, any individual whose data or personal information has been compromised is notified if required, and kept informed throughout the investigation, with a full report being provided of all outcomes and actions.

9.2 Breach Notification

MannionDaniels understands that we have obligations and a duty to report data breaches in certain instances. All staff are aware of these circumstances and we have strict internal reporting lines to ensure that data breaches falling within the notification criteria are identified and reported without undue delay.

9.2.1 Supervisory Authority Notification

When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, we will always communicate the personal data breach to the data subject without undue delay, in a written format and in a clear and legible format.

The notification to the Data Subject shall include: -

- The nature of the personal data breach
- The name and contact details of our DPO and/or any other relevant point of contact (for obtaining further information)
- A description of the likely consequences of the personal data breach
- A description of the measures taken or proposed to be taken to address the personal data breach (including measures to mitigate its possible adverse effects)

We reserve the right not to inform the data subject of any personal data breach where we have implemented the appropriate technical and organisational protection measures which render the data unintelligible to any person who is not authorised to access it (i.e. encryption, data masking etc) or where we have taken subsequent measures which ensure that the high risk to the rights and freedoms of the data subject is no longer likely to materialise. If informing the data subject of the breach involves disproportionate effort, we reserve the right to instead make a public communication whereby the data subject(s) are informed in an equally effective manner.

9.3 Record Keeping of Data Breach records

All records and notes taken during the identification, assessment and investigation of the data breach are recorded and retained for a period of 6

years from the date of the incident. Incident forms are to be reviewed monthly by Senior Management team to assess for patterns or breach reoccurrences and actions taken to prevent further incidents from occurring.

10 Annexes

10.1 Annex 1 Exemptions

It is assumed that all personal information collected and processed by MannionDaniels is subject to the DPA18 and GDPR. However, in some circumstances, such as there is some public interest involved, data may not be affected by the act.

The exemptions can be complex and have particular conditions attached to them. Entitlement to an exemption depends in part on the purpose for processing the personal data in question and each exemption should be considered on a case-by-case basis because the exemptions only permit a departure from the Act's general requirements to the minimum extent necessary to protect the particular functions or activities the exemptions concern.

Should an exemption apply please refer to the ICO website:

DPA 18:

<http://www.legislation.gov.uk/ukpga/2018/12/part/2/chapter/3/crossheading/exemptions-etc/enacted>

GDPR:

<https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/exemptions/>

10.2 Annex 2 European Economic Area (EEA)

The Eight Principle of the Data Protection Act states that personal data shall not be transferred to a country or territory outside the European Economic

Area (EEA), unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The EEA consists of the member states of the European Union together with Iceland, Liechtenstein and Norway.

Providing you are satisfied that you have complied with the other provisions (and the principles) of the DPA, there are no additional restrictions on the transfer of personal data to EEA countries.

The EEA countries are currently the EU countries plus Iceland, Liechtenstein and Norway:

Austria	Germany	Malta
Belgium	Greece	Netherlands
Bulgaria	Hungary	Norway
Croatia	Iceland	Poland
Cyprus	Ireland	Portugal
Czech Republic	Italy	Romania
Denmark	Latvia	Slovakia
Estonia	Liechtenstein	Slovenia
Finland	Lithuania	Spain
France	Luxembourg	Sweden
		United Kingdom

Which countries have an adequate level of protection?

The European Commission has decided that certain countries have an adequate level of protection for personal data. Currently, the following countries are considered as having adequate protection.

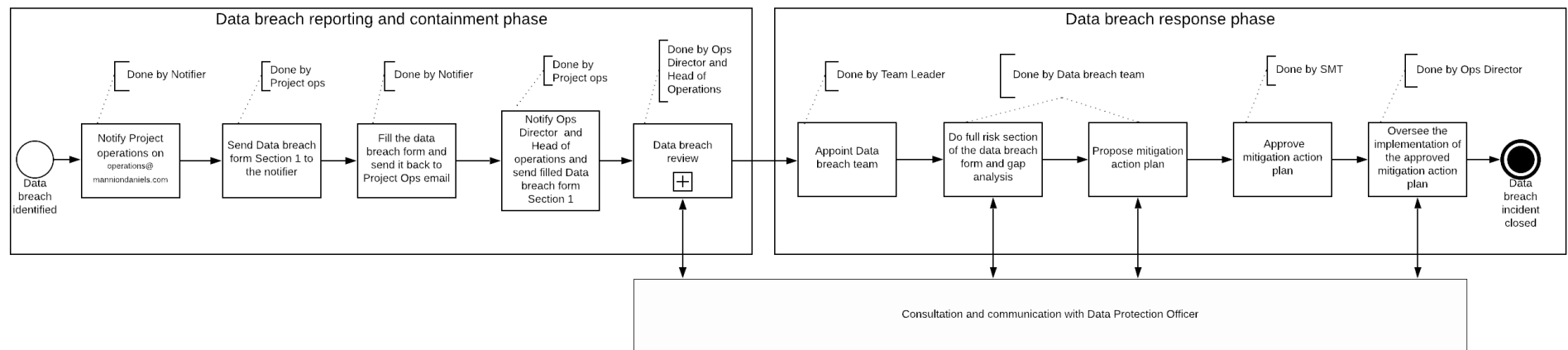
Andorra	Guernsey	New Zealand
Argentina	Isle of Man	Switzerland
Canada	Israel	Uruguay
Faroe Islands	Jersey	

View an up to date list of such countries on the European Commission's data protection website.

Unless absolutely necessary data should not be transferred outside of the EEA, should it be deemed necessary the person responsible shall ensure that appropriate security measures are taken.

10.3 Annex 3 Data Breach Procedure

Data Breach Process Map - High level



10.4 Annex 4 Data Breach Incident Form

SECTION 1: Incident information (filled by a person who discovers the breach)	
Name:	
Position:	
Email:	
Describe as much as you can about what happened, what went wrong and how it happened?	
How did you find out about breach?	
Time and date when you discovered data breach	
Time and date when data breach happened	
Categories of personal data included in breach (see list of categories at the end of the form)	
Categories of data subjects effected (see list of categories at the end of the form)	

Number of personal data records concerned			
Number of data subjects could be affected			
Data breach was caused by a cyber incident	YES	NO	I DO NOT KNOW
List all staff involved in breach:			
List all procedures involved in breach:			
List all third parties involved in breach:			
Describe potential impact on data subject as a result of the breach:			
Please state if there has been any actual harm to data subject:			

Categories of personal data included in the breach:

- 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)

Categories of data subjects:

- Employees
- Users
- Subscribers
- Students
- Customers or prospective customers
- Patients
- Children
- Vulnerable adults
- Not yet known
- Other (please, give details)

SECTION 2: Containment and reporting (filled by Ops team):		
Name of Operations Director:		
Email of Operations Director:		
Name of DPO:		
Email of DPO:		
What is the immediate action taken to contain breach?		
What is the root cause of breach?		
Data breach is a high risk to the rights and freedoms of an individual	YES	NO
There is a significant delay between data breach and breach reporting	YES	NO
If there is a significant delay in reporting, explain why.		

The supervisory authority was already notified	YES	NO
The supervisory authority was notified within 72 hours since data breach	YES	NO
If there is a delay in reporting to the supervisory authority, explain why.		
Data subject was notified?	YES	NO

SECTION 3: Cyber incidents (filled by Head of IT department):

Head of IT department:			
Email:			
The confidentiality of your system has been affected	YES	NO	I DO NOT KNOW
The integrity of your system has been affected	YES	NO	I DO NOT KNOW
The availability of your system has been affected	YES	NO	I DO NOT KNOW
Describe the impact of the cyber incident on MannionDaniels (circle the most appropriate answer)			
High	MD have lost the ability to provide all critical services to all users		
Medium	MD have lost the ability to provide a critical service to some users		
Low	There is no loss of efficiency, or a low loss of efficiency, and MD can still provide all critical services to all users		
Not yet known			
Describe the recovery time from the incident (circle the most appropriate answer)			
Regular	IT can predict recovery time with the existing resources		
Supplemented	IT can predict recovery time with the additional resources		
Extended	IT cannot predict recovery time and need extra resources		
Not recoverable	Recovery from the incident is not possible, e.g. backups cannot be restored		
Complete	Recovery is complete		
Not yet known			

4: Data breach response (filled by Operations team):		
Name of Operations Director:		
Email:		
Risk assessment –		
State the possible outcomes / results of a data breach (impact and probability) Use risk impact and risk probability categories from risk management policy		
Significant contributors to the data breach		
State actions to take to avoid this breach happen again		
Describe any steps (in outline) MD is taking to minimise the recurrence of data breach – mitigation plan		
Implementation of a mitigation require controlled change	YES	NO
Date mitigation plan approved by the Leadership team		
Person appointed to oversee the implementation of a mitigation plan		
Name:		
Email:		

10.5 Annex 5 Disposal/retention criteria checklist

	Location, format and purpose of data is clearly defined.
	Data type and its retention period is clearly defined in the retention guideline or in any related contractual requirements.
	MannionDaniels will not require data in the future. (i.e. future reference purposes, training, precedents, performance management, performance

	indicators, benchmarking, comparison exercises, for its historical or intrinsic value, etc.)
	Data is free of inclusion in any litigation, claim or dispute.

If there is any doubt in any of the answers, you must contact Operations Director or Data Protection Officer.

10.6 Annex 6 Retention Guidelines

This table relates to both electronic and paper storage and is based on statutory requirements where stipulated. Where the recommended retention period given is 6 years or longer it is based on the 6-year time limit within which legal proceedings must be commenced as laid down under the Limitation Act 1980. Please, check also the contractual requirements which might differ from retention guidelines. If the disposal / retention criteria differ from contractual requirements, it is important the longer retention period is always respected.

Document type	Retention limit	Legislation (where known)
Accounting records detailing company transactions, including supporting documents	3 years from creation date – private company 6 years from creation date – public company	Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006
Formal company documents such as statutory books, board minutes, resolutions	Indefinitely	
Company/board meeting minutes	10 years from date of meeting	
Payroll and wage records	6 years from end of financial year	Taxes Management Act 1970
Income tax and NI returns, income tax records and correspondence with HMRC	Not less than 3 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993(SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631)
Job applications and interview records	Up to a year	
Evidence of the right to work	2 years after employment ceases	Immigration, Asylum and Nationality Act 2006
Personnel and training records	Up to 6 years after employment ends	
Employee bank records	No longer than necessary	
Personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases	
Retirement Benefits Schemes – records of notifiable events, for example, relating to incapacity	6 years from the end of the scheme year in which the event took place	The Retirement Benefits Schemes (Information Powers) Regulations 1995(SI 1995/3103)
Statutory Maternity Pay records	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986(SI 1986/1960) as amended

Document type	Retention limit	Legislation (where known)
Parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance	
Pension scheme investment policies	12 years from the ending of any benefit payable under the policy	
Pensioners' records	12 years after benefit ceases	
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy	
Statutory Sick Pay records, calculations, certificates, self-certificates	6 years after employment ceases	
VAT records	6 years	Value Added Tax Act 1994
Corporation tax records: Company assets (e.g. receipts, sales and purchases) Company liabilities Income and expenses Tax deduction or tax credit vouchers	6 years (min.) from end of accounting period, longer if returns are late	
Accident books, accident records/reports	3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR)(SI 1995/3163) as amended, and Limitation Act 1980
Assessments under health and safety regulations and records of consultations with safety representatives and committees	Indefinitely	
Medical records and details of biological tests under the Control of Lead at Work Regulations	40 years from the date of the last entry	The Control of Lead at Work Regulations 1998(SI 1998/543) as amended by the Control of Lead at Work Regulations 2002 (SI 2002/2676)

Document type	Retention limit	Legislation (where known)
Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)	40 years from the date of the last entry	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
Medical records under the Control of Asbestos at Work Regulations	40 years from the date of the last entry	The Control of Asbestos at Work Regulations 2002 (SI 2002/ 2675). Also see the Control of Asbestos Regulations 2006 (SI 2006/2739) and the Control of Asbestos Regulations 2012 (SI 2012/632)
Medical records under the Ionising Radiations Regulations 1999	Until the person reaches 75 years of age, but in any event for at least 50 years	The Ionising Radiations Regulations 1999(SI 1999/3232)
Records of tests and examinations of control systems and protective equipment under the Control of Substances Hazardous to Health Regulations (COSHH)	5 years from the date on which the tests were carried out	The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677)
Records relating to a specific property including maintenance and estate planning	7 years after property no longer occupied	
CCTV recordings	4 weeks from the date recorded except where required as evidence	
National Minimum wage records	3 years after the end of the pay reference period following the one that the records cover	National Minimum Wage Act 1998
Records relating to working time	2 years from which date on which they were made	The Working Time Regulations 1998 (SI 1998/1833)

Where there is no definitive retention period defined, Operations Director or Data Protection Officer must be contacted to clarify.

Document type	Recommended Retention limit
Actuarial valuation reports	Permanently
Application forms, CVs and interview notes for unsuccessful candidates	1 year
Inland Revenue/HMRC approvals	Permanently

Document type	Recommended Retention limit
Money purchase details	6 years after transfer or value taken
Senior executives' records (that is those on a senior management team or their equivalents)	Permanently for historical purposes
Time cards	2 years after audit
Trust deeds and rules	Permanently
Trustees' minute books	Permanently
Works council minutes	Permanently

10.7 Annex 7 Possible data breach responses

In the event of data breach following breach responses might be considered

Human error

- Re-training in specific/all compliance areas
- Re-assessment of compliance knowledge and understanding
- Suspension from compliance related tasks
- Formal warning (in-line with the MannionDaniels disciplinary procedures)

System error


- Attempting to recover any lost equipment or personal information
- Shutting down an IT system
- Removing an employee from their tasks
- The use of back-ups to restore lost, damaged or stolen information
- Making the building secure
- If the incident involves any entry codes or passwords, then these codes must be changed immediately, and members of staff informed


10.8 Annex 8 Personal Data flow diagrams

10.8.1 How to read the diagrams

10.8.1.1 Personal Data source

The flow of information starts either at the data subject with the

following sign  (person icon in green colour) or organisation which is

providing personal data (data controller) with the following sign  (square shape with the white fill and green borderline). One diagram can have more than one source of personal data, therefore, more than one starting point.

10.8.1.2 Data processing

There are several types of data processing channels used in the diagrams such as;

- Data reception indicated by the green line.
- Data internal processing within MannionDaniels, indicated by the black line.
- Data sharing with the external providers or systems, indicated by the yellow line.
- Data disposal from MannionDaniels managed locations, indicated by the red line. The data disposal is indicated on the specific diagrams of sub-processes; however, it is not indicated on the master diagram.

If necessary, data processing channels are enriched by the additional comments to bring more clarity to the extent of data processing, data type and conditions of processing.

10.8.1.3 Direction of flow data

The arrow always indicates the direction of data flow. It is possible that one data access servers for data reception and data provision in which case arrows are placed at both directions of the processing.

The start of the personal data flow starts with the data subject or organisation providing data (indicated by green colour) continues possibly to all directions of data processing and ends with the partner or partner organisation which MannionDaniels shares data with (indicated by yellow colour)

10.8.1.4 Icons and shapes used in the diagrams



(the circle shape with the white fill and black borderline)

- The shape indicates data processing by the specific team within MannionDaniels. The description of the team is always placed in the circle



(the cloud shape with white fill and black borderline)

- The shape indicates cloud-based systems and services used in data processing where MannionDaniels is in control of data management. The name of the service provider or name of the system is always described in the shape together with the branding icon.



(the cloud shape with yellow fill and black borderline)

- The shape indicates cloud-based systems and services used in data processing where MannionDaniels is not in control of data management. The name of the service provider or name of the system is always described in the shape together with the branding icon.



(the square shape with yellow fill and black borderline)

- The shape indicates partners and organisations which MannionDaniels shares personal data. The partners or organisations are responsible for data management and agreed to adhere to the GDPR. The name of the organisation is described in the shape together with the branding icon. The type of the partners is described by the text description in the shape.



(the square shape with white fill and red borderline)

- The shape indicates data disposal. The shape is used in all sub-processes' diagrams but not in the master diagram.



(open bracket)

- The shape indicates a description of the data type for the specific data processing channel. For more clarity, the connection between the data type description and channels is represented by the dotted line.



(the cylinder shape with white fill and black borderline)

- The shape indicates MannionDaniels server. The description of the specific systems is described by the text inside of the shape.



(the square shape with white fill, USB sign in black colour and 'USB driver' text inside of the shape)

- The shape indicates the use of USB drives for storing and transfer of personal data.



(the laptop icon with a blue fill)

- The icon indicates the use of the laptop for storing personal data.



(the 'house like shape' with white fill and black borderline)

- The shape indicates



(the inverted 'house like shape' with white fill and black borderline)

10.8.2 List of application, systems and services in use

- BOX – cloud-based data storage system
- MS Outlook – email delivery system with data stored on third-party servers
- People HR – cloud-based HR system with some bespoke capabilities
- MimeCast – email delivery system with data stored on third-party servers
- SAGE – accountancy system with data stored on MD server
- SMILE – Bespoke fund management cloud-based system
- Dow Jones – cloud-based news database services
- Fraud checker – documents fraud checker with data stored on MD server
- Get response – cloud-based online communications system
- Replicon – cloud-based data storage system
- OneDrive – cloud-based data storage system
- Google Drive cloud-based data storage system
- Smartsheet – collaboration and work management web application

10.8.3 List of banking systems in use

- Handelsbanken
- Western Union

- Stanbic Bank
- Zenith
- Other correspondent banks

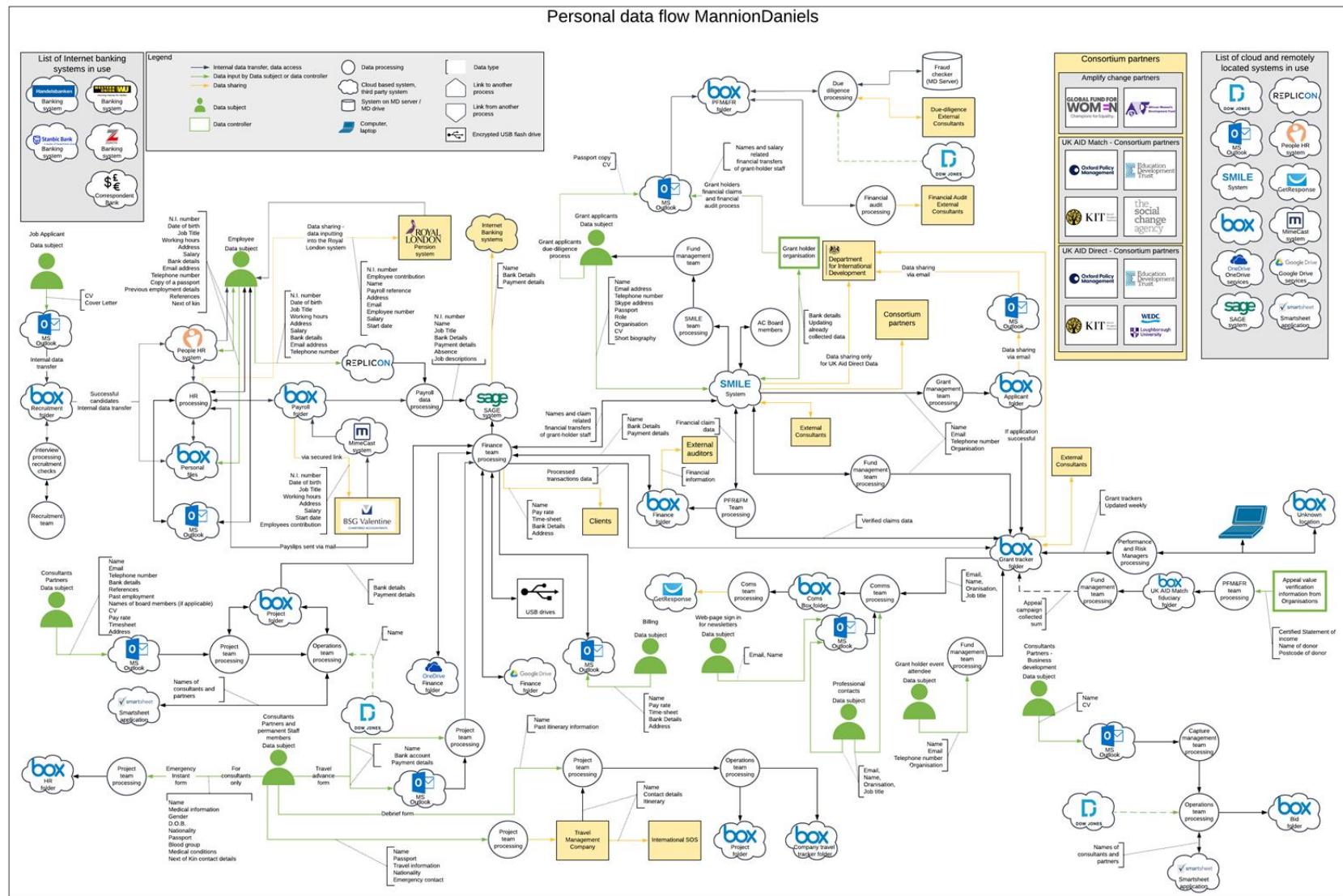
10.8.4 List of Consortium Partners

- Global Fund for Women
- African Women's Development Fund
- Oxford Policy Management
- Education Develop Trust
- KIT – Royal Tropical Institute
- The Social Change agency
- WEDC Loughborough University

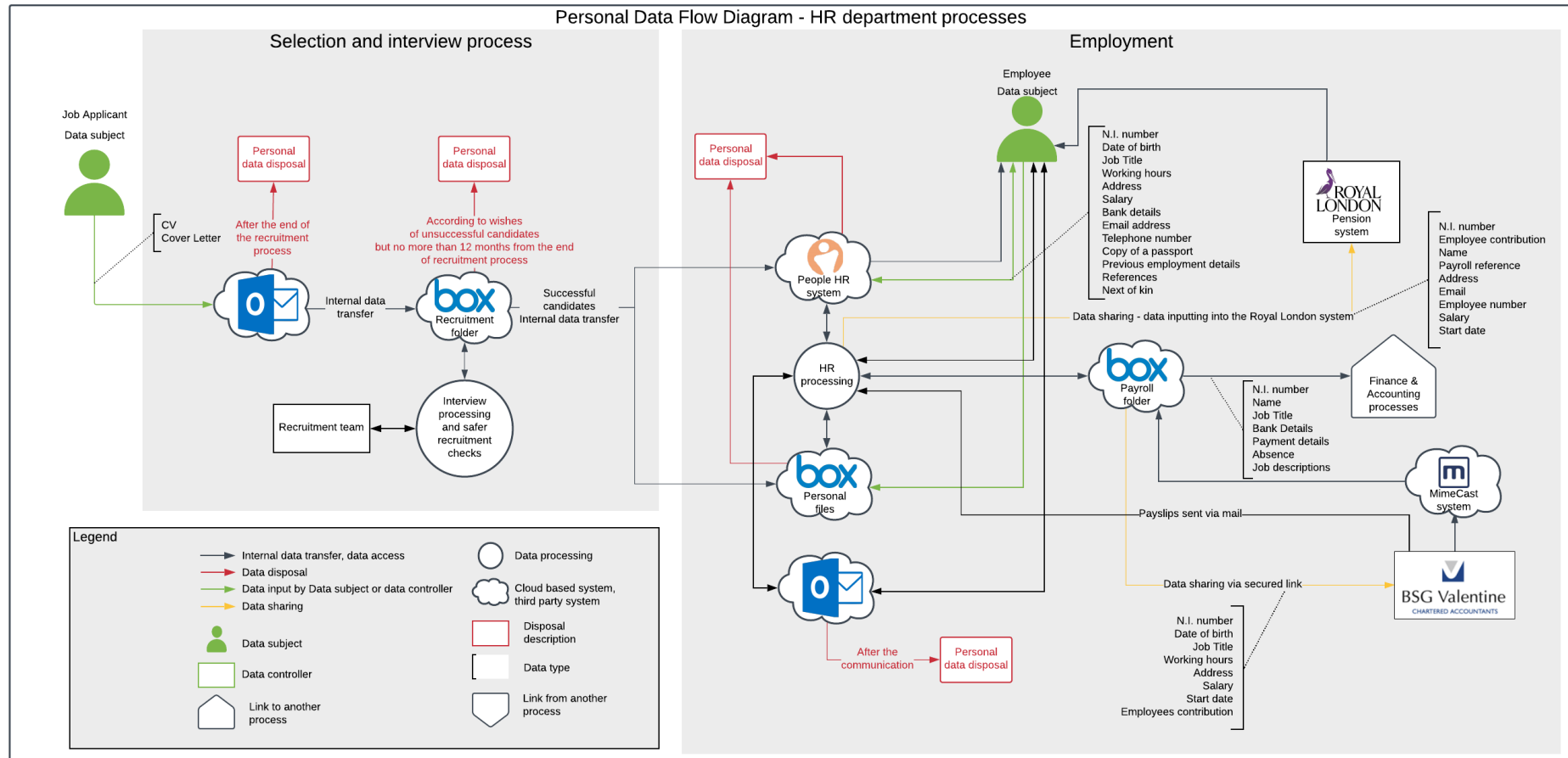
10.8.5 List of other partners and service providers

- Department for International Development
- Royal London
- BSG Valentine

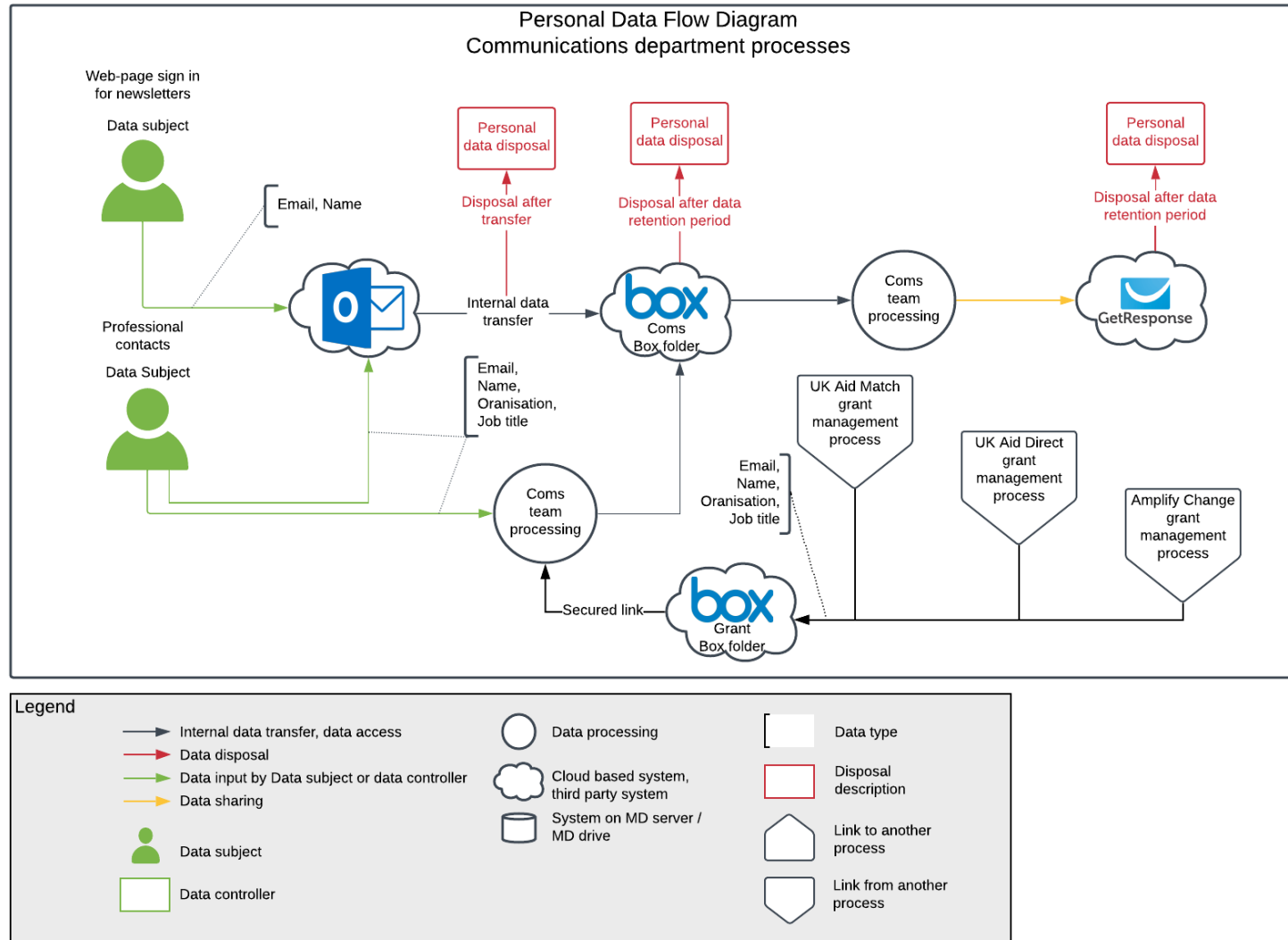
10.8.6 Master personal data flow diagram



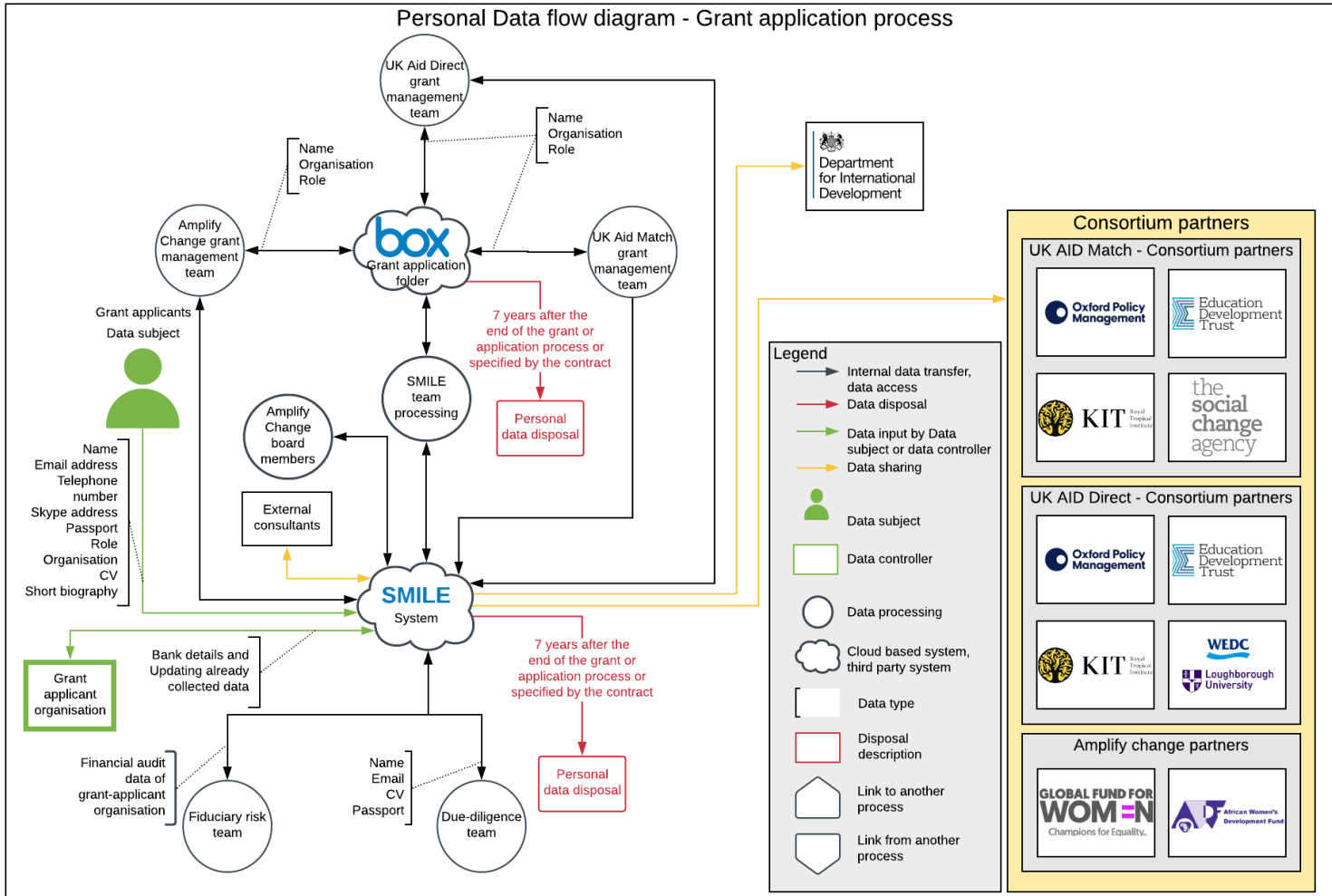
10.8.7 HR department processes personal data flow diagram



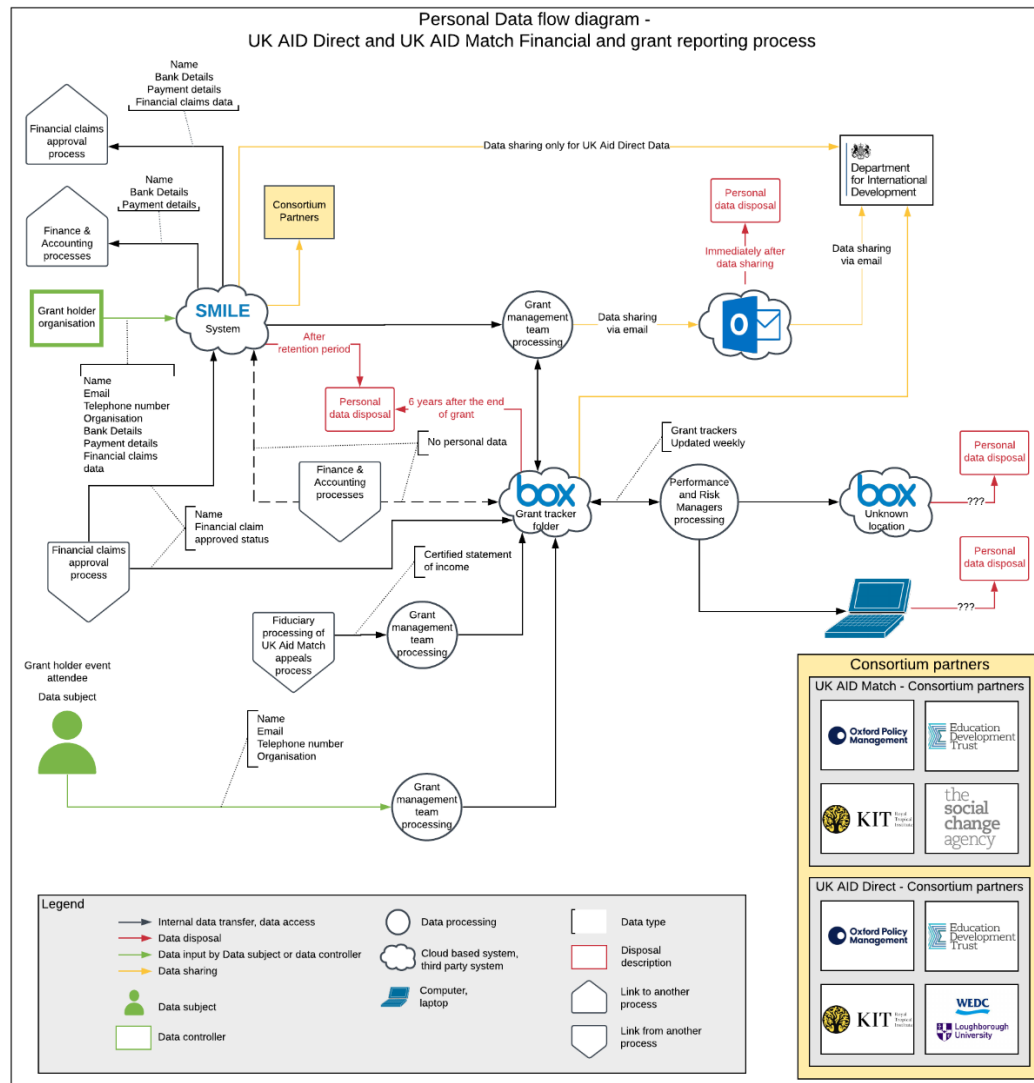
10.8.8 Communications department processes personal data flow diagram



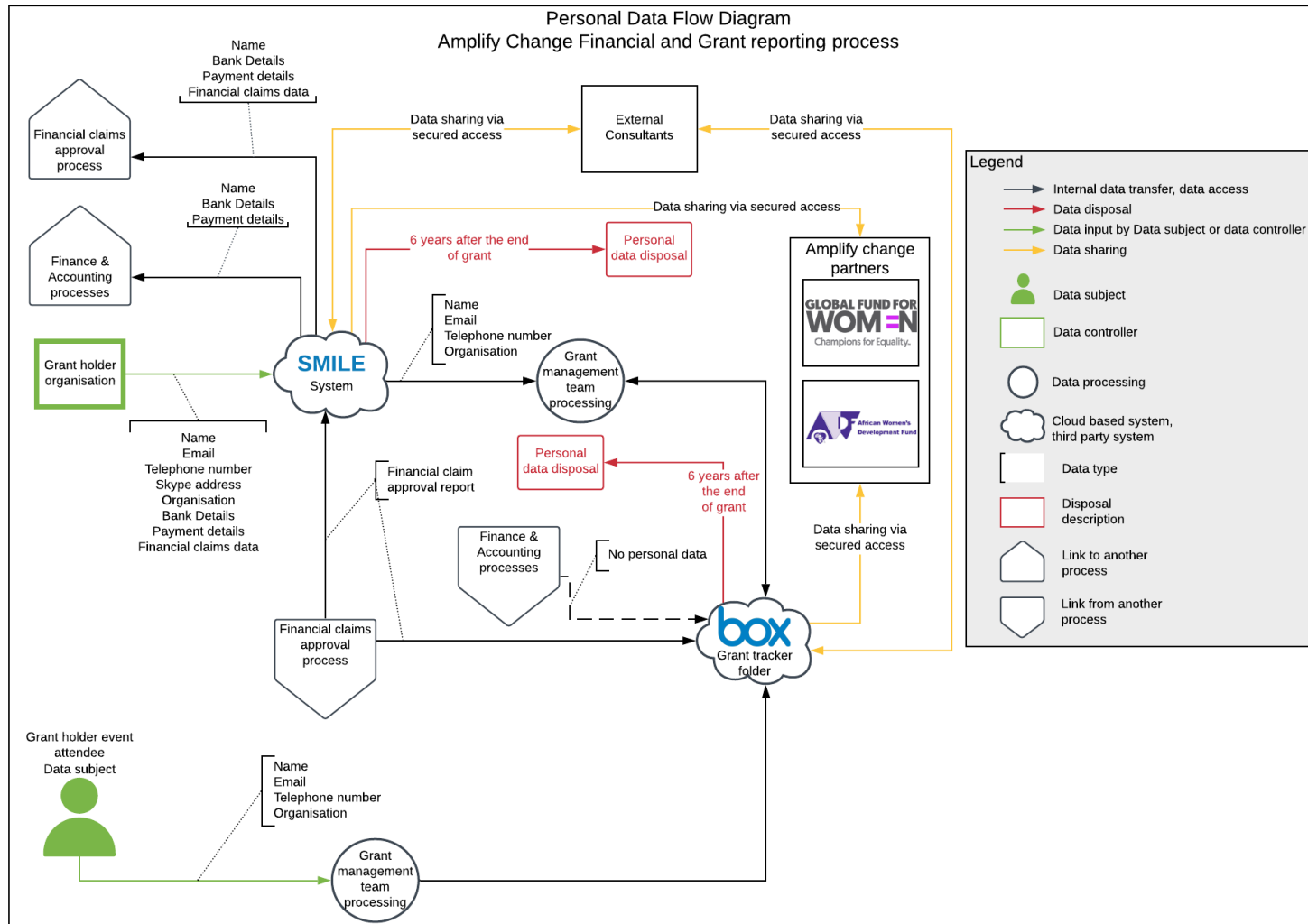
10.8.9 Grant application process personal data flow diagram



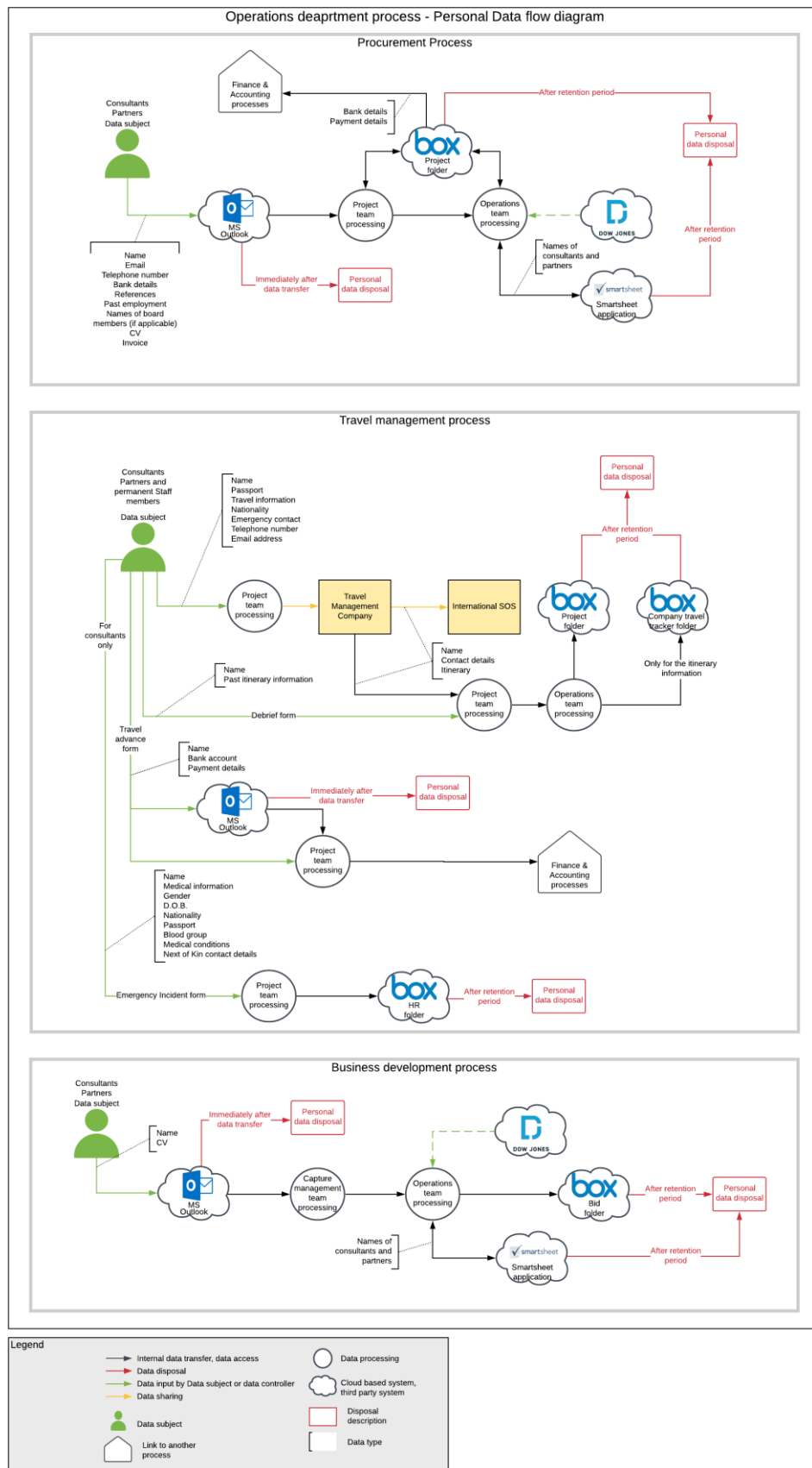
10.8.10 UK Aid Match & UK Aid Direct processes personal data flow diagram



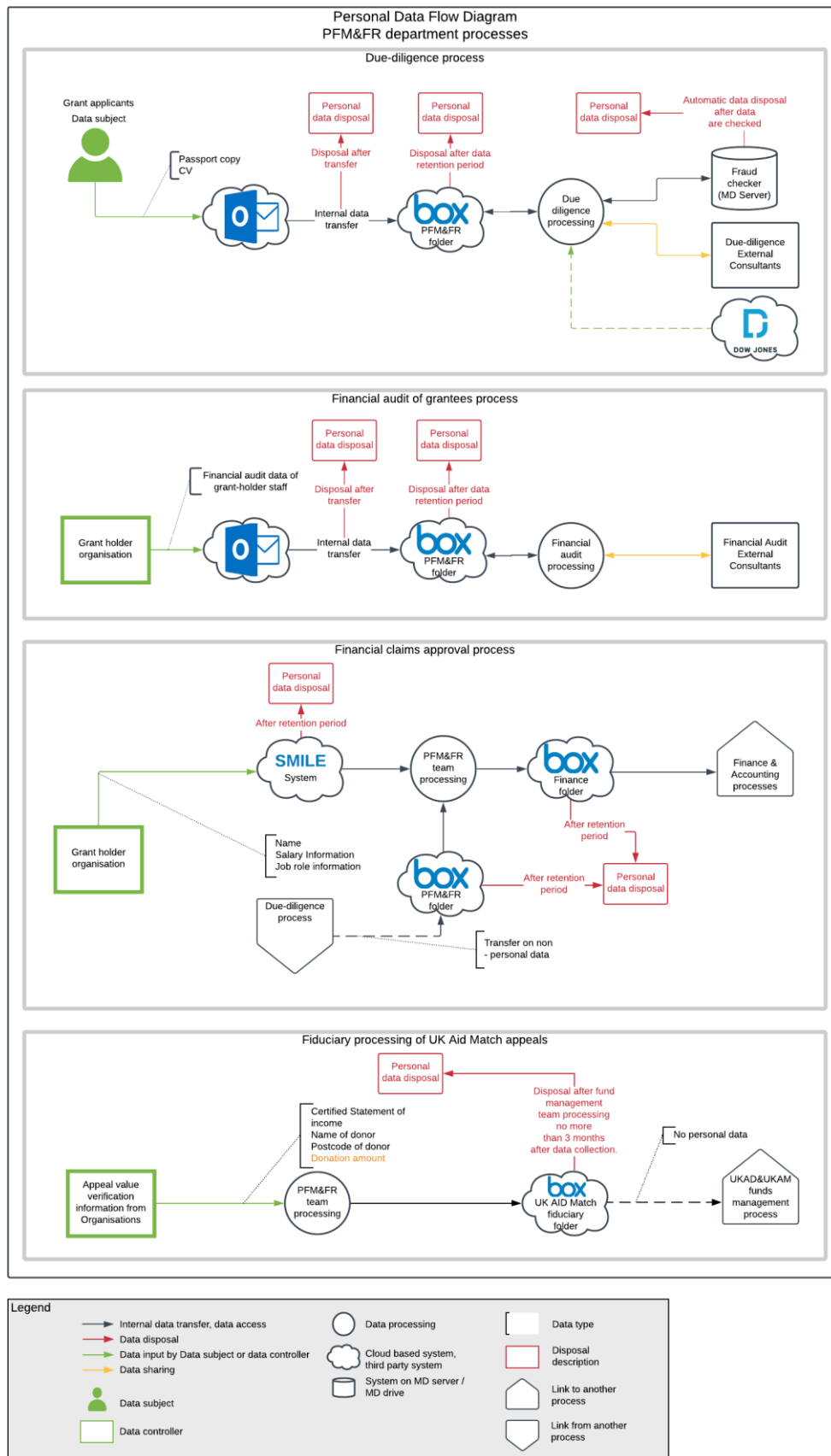
10.8.11 Amplify change processes personal data flow diagram



10.8.12 erations department processes personal data flow diagram



10.8.13 PRM&FR department processes personal data flow diagram



10.8.14 Finance department processes personal data flow diagram

