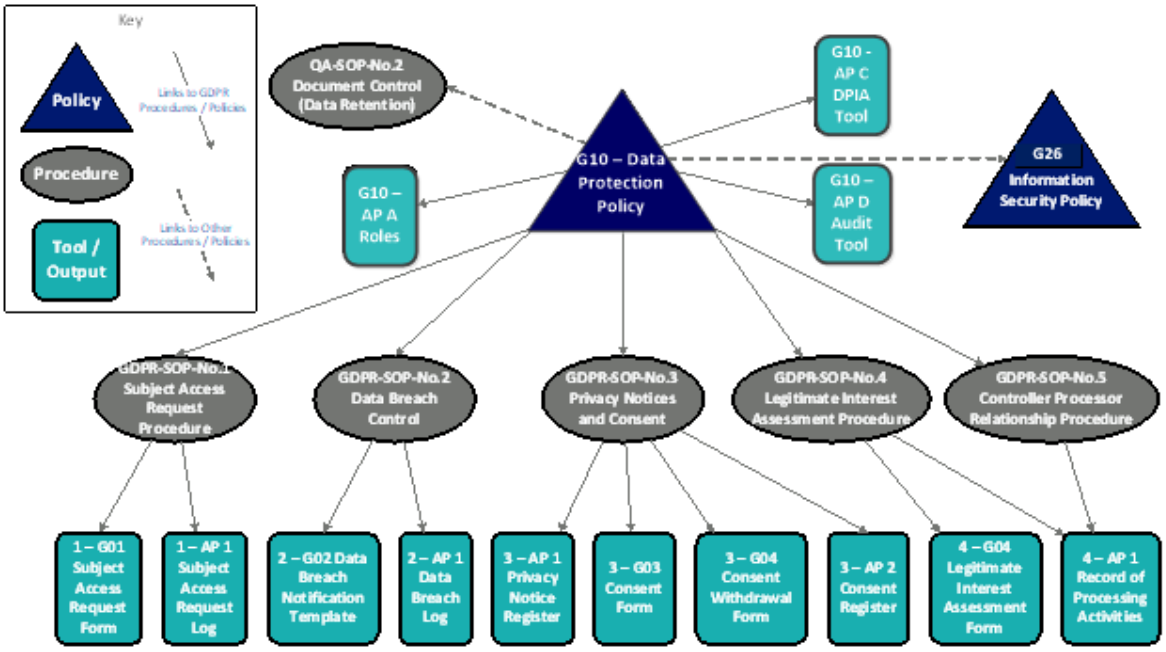
WILSON JAMES POLICY STATEMENT

Policy Title	GDPR Data Protection Policy	**Policy No.**	G10
Owner	Information Security Management Forum	**Date Issued**	Jul-07
Author	Information Security & Compliance Manager	**Date Reviewed**	Jan-20
Scope	This Policy applies to all sectors and functions of the Wilson James business, all 'workers' and all geographic territories in which Wilson James operates		
Responsibility	The Policy owner is responsible for ensuring that this policy remains current and up to date and shall formally review the policy on an annual basis		

Foreword and Scope

A glossary of GDPR terms can be found in Appendix 1 toward the end of the policy. These terms are tagged with [A] when first used.

There are a several procedures and tools that have been developed in conjunction with this GDPR Data Protection Policy. Together, they make up the Personal Information Management System for Wilson James. The structure of this Policy Suite is as follows and a larger version of this diagram, without the document reference numbers can also be found in Appendix 2:



The procedures and tools are referenced throughout this policy document.

Introduction

Wilson James' objectives for the policy suite are:

- Support organisational objectives
- Impose controls in line with Wilson James' acceptable level of risk
- Meet applicable statutory, regulatory, contractual and professional duties
- Protect the interests of individuals and other key stakeholders.

WILSON JAMES POLICY STATEMENT

The Board of Directors at Wilson James are committed to compliance with all relevant UK and EU laws in respect of personal data[A], and believe that workers (employees, contractors, agency staff), clients and suppliers have a right to expect that information held regarding them will be processed carefully, with confidentiality in mind. To protect the "rights and freedoms" of individuals, this Data Protection Policy has been written in accordance with the General Data Protection Regulation (GDPR). The legislation outlines how Wilson James can ensure that personal data is collated and used fairly, stored safely, and not disclosed to any other person or party unlawfully.

The policy applies to all workers and interested parties of Wilson James such as outsourced suppliers. Any breach of the GDPR will be dealt with under Wilson James' disciplinary policy and may also be a criminal offence, in which case the matter will be reported to the appropriate authorities.

Partners and third parties working with or for Wilson James, who may have access to personal information, will be expected to read, understand and comply with this policy. No third party may access personal data held by Wilson James without having first entered into a data confidentiality agreement, which imposes compliant standards of conduct and which gives Wilson James the right to audit compliance with the agreement.

If you have any queries or concerns about the application of this Data Protection Policy, please contact dataprotection@wilsonjames.co.uk for advice and guidance.

GDPR Summary

GDPR applies to the handling of personal data. The majority of personal data held about a worker is held at the Support Centre and forms an individual's personnel file or electronic payroll file. In addition, personal data may be held about client and supplier contacts, such as email address, phone number, preferences, job role and location.

The key is to remember that personal data covers both facts and opinions about an individual and can also include information regarding the intentions of the data controller towards that individual.

In addition to personal data, GDPR also defined 'Special categories[A] of personal data' which are subject to higher controls. Special categories include personal data about ethnicity, political opinions, religious or philosophical beliefs, trade-union membership, genetic or biometric data, data concerning health or data concerning a natural person's sexual orientation.

Wilson James is committed to complying with data protection legislation and good practice. By extension, this means that any worker processing[A] data regarding Wilson James workers, clients or suppliers must comply with the following 6 GDPR principles. Personal data must be:

1. Fairly and lawfully processed
2. Processed only for explicit and legitimate purposes
3. Adequate and relevant and not excessive, in relation to the purpose for which is it collected
4. Kept accurate and where necessary, up to date
5. Retained for only as long as required for regulatory or legitimate organisational purposes
6. Kept secure.

In addition to the principles, Wilson James will also adhere to the following:

- Provide clear information to individuals about how their personal information will be used and by whom
- Maintain a record of the categories of personal information processed by Wilson James

- Notify the Information Commissioner's Office that Wilson James is a data controller[A] and the GDPR Owner will review this notification annually;
- Respect individuals' rights in relation to their personal information, including their right of access
- Only transfer personal information outside the EU in circumstances where it can be adequately protected
- Notify the Information Commissioner's Office of personal data breaches[A] without undue delay
- Document the roles and accountabilities for the governance of Wilson James' personal data
- Manage risk and carry out mandatory Data Protection Impact Assessments (There is a section on DPIAs later in this policy)
- Apply various exemptions allowable by data protection legislation.

Roles and Responsibilities under the GDPR

The Board of Directors and all those in managerial or supervisory roles throughout Wilson James are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.

The GDPR draws a distinction between a data controller and a data processor[A] in order to recognise that not all organisations involved in the processing of personal data have the same degree of responsibility. The data controller is ultimately responsible for ensuring that all personal data is kept securely and in compliance with the regulation. GDPR also emphasises accountability which means that the controller is not only responsible for ensuring compliance but also needs to be able to effectively demonstrate that compliance with relevant documented evidence or audit trail.

Wilson James has the role of data controller in relation to personal data that it collects, owns and makes decisions about. An example of this would be information about Wilson James' own workers. Operational arms of Wilson James may collect and manage personal data on behalf of clients; data that clients make decisions about. In this context, Wilson James is a data processor and the client is the data controller.

The GDPR defines the role of Data Protection Officer which is mandatory for some organisations. This role is not mandatory for Wilson James, but there are several other GDPR-related roles which are defined in a separate document called G10 - AP A Roles that will undertake similar responsibilities. The GDPR Owner role currently sits with the Chief Information Officer. This role will determine the standard for relationships between controllers and processors, using the GDPR-SOP-No.5 Controller Processor Relationship Procedure and will monitor and evidence compliance with the GDPR.

The GDPR Owner is accountable to Board of Directors. This accountability also includes information security and risk management in relation to compliance with this policy.

The Data Manager role report to the GDPR Owner and has specific responsibilities in respect of procedures such as the Subject Access Request Procedure (See GDPR-SOP-No.1 Subject Access Request Procedure document) and are the first point of call for workers seeking clarification on any aspect of data protection compliance.

Compliance with data protection legislation and adherence to the GDPR Data Protection Policy is the responsibility of every Wilson James worker. Any breach of this policy, whether deliberate or as a result of negligence, exposes Wilson James and individual workers to risk and may lead to disciplinary action.

It is also the worker's responsibility to ensure that any information they provide in connection with their employment is accurate and up to date. This is a condition of each worker's employment.

WILSON JAMES POLICY STATEMENT

GDPR Training Policy
GDPR is elevating the importance of Data Protection to a similar level as Health and Safety. Awareness and training of all staff handling data is mandatory and as such, the training policy for GDPR will match that of training for Health and Safety in the workplace. Basic GDPR training will form part of the induction programme for all Wilson James workers, and this training will be refresh every 2 years.

Information Risk Management
Wilson James has a process for assessing risks relating to the processing of personal data. Strategic level risks are documented on the corporate risk register which are owned by the GDPR Owner and reviewed by the Board of Directors monthly. Mitigating activities are planned by the GDPR Owner, to reduce these risks to an acceptable level.

Wilson James also has a procedure for assessing operational risks to individuals associated with the processing of their personal information. Where a type of processing (in particular using new technologies) is likely to result in a high risk to the "rights and freedoms" of data subjects[A], Wilson James shall, prior to the processing, carry out an assessment of the impact on the protection of personal data. This is called a Data Protection Impact Assessment (See G10 – AP C DPIA Tool). A single assessment may address a set of similar processing operations that present similar high risks.

Where the Data Protection Impact Assessment identifies that processing of personal information could cause damage and/or distress to the data subjects, the decision whether to proceed must be escalated for review to the GDPR Owner. The GDPR Owner may in turn, escalate the matter to the Information Commissioner's Office.

Appropriate security controls may be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level, by reference to Wilson James' documented risk acceptance criteria and the requirements of the GDPR.

The 6 GDPR Principles
All processing of personal data must be done in accordance with the 6 principles of the Regulation, and Wilson James' policies and procedures are designed to ensure compliance with them.

<u>Principle 1 – Personal data must be processed lawfully, fairly and transparently.</u>
The GDPR introduces the requirement for transparency whereby the Data Controller must communicate certain information to the data subject at the point where their data is captured. This must be done using clear and plain language and must as a minimum include:

- The identity and the contact details of the data controller
- The intended purposes of processing the personal data, as well as the legal basis
- How long the personal data will be stored
- The existence of the data subject's 8 rights, including the right to request access, rectification, erasure or to object to processing
- The categories of personal data concerned
- The categories of recipients[A] of the personal data, (where applicable)
- Whether the controller intends to transfer personal data to a recipient in a third country
- Any further information necessary to guarantee fair processing.

The GDPR-SOP-No.3 Privacy Notice and Consent Procedure provides more detail and the Privacy Notices themselves are published on the Wilson James website and hard copies are also available. These should be clearly sign-posted to all data subjects at the point where their personal data is collected.

In addition to this, Wilson James must document the lawful reasons for processing personal data in the 4 – AP 1GDPR Record of Processing Activities. The 6 allowable lawful reasons are:

1. Data subject consent
2. For the performance of a contract in which the data subject is a party
3. Legal obligation
4. To protect the vital interests of a data subject
5. Tasks carried out in the public interest
6. Legitimate interests pursued by the controller or by a third party

Further guidance about the lawful basis for processing and how to establish 'Legitimate Interests' can be found in the GDPR-SOP-No.4 Legitimate Interest Assessment Procedure.

Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes

Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of Wilson James' GDPR registration, or those purposes communicated to the data subject within the privacy notice. For any deviations to these purposes, the GDPR Owner must be informed and determine whether additional consent[A] must be captured, from the Data Subjects.

The consent procedure is described in GDPR-SOP-No.3 Privacy Notices and Consent Procedure.

Principle 3 - Personal data must be adequate, relevant and limited to what is necessary for processing

The GDPR Owner is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected. All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must be approved by the GDPR Owner.

The data collection methods are reviewed on an annual basis to ensure that collected data continues to be adequate, relevant and not excessive.

By using the G10 – AP C DPIA Tool when there are significant changes to the way data is processed, Wilson James are ensuring that data minimisation and therefore risk minimisation is designed into data processes on an ongoing basis.

Principle 4 - Personal must be accurate and kept up to date

Data that is kept for a long time must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

The HR Director is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

It is also the responsibility of individuals to ensure that data held by Wilson James is accurate and up-to-date. Completion of an appropriate registration or application form will be taken as an indication that the data contained therein is accurate at the date of submission.

Wilson James workers, suppliers and customers should notify Wilson James of any changes in circumstance to enable personal records to be updated accordingly by using their usual business contact point or email dataprotection@wilsonjames.co.uk. It is the responsibility of Wilson James to ensure that any notification regarding change of circumstances is noted and acted upon.

The GDPR Owner is also responsible for ensuring that rectification requests are passed onto any third-party organisations that have been a recipient of that personal data as part of normal business processes.

The Data Manager will regularly review personal data, by reference to the GDPR Record of Processing Activities, to identify any data quality issues. The Data Manager is responsible for ensuring that appropriate additional steps are taken to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

Principle 5 - Personal data must be kept (in a form that identifies a data subject) only as long as is necessary, for processing

Personal data may not be retained for longer than it is required. Once a member of staff has left Wilson James, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. Wilson James' Data Retention Rules are documented in QA-SOP-NO.2 and will apply in all cases, and once its retention date is passed, data must be securely destroyed (e.g. shredding, disposal as confidential waste, secure electronic deletion).

The GDPR Owner must specifically approve any data retention that exceeds the retention period defined in Data Retention Rules and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation. This approval must be written.

Where personal data is retained beyond the processing date, it will be minimised / encrypted / pseudonymised in order to protect the identity of the data subject in the event of a data breach.

The GDPR Owner is responsible for ensuring that all personal data is collected, retained and destroyed in line with the requirements of the GDPR, but relevant Directors / Heads of department are responsible for ensuring their area of the business incorporates Data Retention Rules into standard business operations.

Principle 6 - Personal data must be processed in a manner that ensures its security

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

These controls are selected based on identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

Wilson James' compliance with this principle is contained in its IT02 - Information Security Policy and in the Cyber Essentials Plus accreditation. These security controls will be subject to audit and review.

Data Subjects' Rights

To reinforce these principles, data subjects have eight rights under GDPR:

1. The right to be informed – about what data is held about them, the purposes for which it is being processed and details of who that data is shared with
2. The right of access – to a copy of information held about them and be told about the sources of the data
3. The right to rectification – if some of the personal data is inaccurate or incomplete
4. The right to erasure – where there is no longer a legal purpose for keeping the data or where a subject withdraws consent
5. The right to restrict processing – for example, where processing is likely to cause damage or distress or prevent processing for purposes of direct marketing.
6. The right to data portability – to a machine-readable copy of personal data that the subject has provided to Wilson James

7. The right to object – to processing based on the grounds of public interest or legitimate interests, or to any automated profiling[A] without consent.
    a. Data subjects may complain directly to Wilson James by contacting dataprotection@wilsonjames.co.uk
    b. Data subjects may also complain directly to or escalate to the UKs supervisory authority[A] - the Information Commissioner's Office.
8. Rights in relation to automated decision making and profiling – where this exists, data subjects can ask for human intervention in the decision-making process, or to be informed of the logic involved in the decision-making process

Data subjects may sue for compensation if they suffer damage by any contravention of the GDPR.

Data subjects may make data access requests as described in GDPR-SOP-No.1 Subject Access Request Procedure. All Wilson James workers should be able to recognise a subject access request and take action according to the procedure. This procedure also describes how Wilson James will ensure that its response to the data access requests is compliant with the requirements of the Regulation.

International Transfers
Personal data shall not be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects. It is prohibited, unless one or more of the specified safeguards or exceptions apply:

- An assessment of the adequacy based on:
    - The nature of the information being transferred and how it will be used
    - Laws and practices of the country of the transferee, including relevant codes of practice and international obligations
    - The security measures that are to be taken as regards the data in the overseas location
    - The country or territory of the origin, and final destination, of the information - a list of countries that satisfy the adequacy requirements of the Commission are published in the Official Journal of the European Union.
- The adoption of approved binding corporate rules[A] for the transfer of data outside the EU. This requires submission to the relevant Supervisory Authority to approve the rules
- The adoption of Model contract clauses - Wilson James may adopt approved model contract clauses for the transfer of data outside of the EU. If Wilson James adopts the model contract clauses approved by the relevant Supervisory Authority, there is an automatic recognition of adequacy.
- In the absence of an adequacy decision, including binding corporate rules, a transfer of personal data to a third country can occur on one of the following exceptions:
    - The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks
    - The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request
    - The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person
    - The transfer is necessary for important reasons of public interest
    - The transfer is necessary for the establishment, exercise or defence of legal claims
    - The transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent

- The transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest

Any decision to transfer data to a new third country should be supported by a completed Data Protection Impact Assessment, using the G10 – AP C DPIA Tool, to evidence that any risks are assessed and addressed. When in doubt, contact the GDPR Owner for advice on the decision-making processes.

Data Protection Impact Assessment (DPIA)

A DPIA is a process which helps an organisation to identify and reduce the privacy risks. DPIAs are now a mandatory requirement under GDPR, when systems or process changes are likely to result in a high risk to the rights and freedoms of natural persons. This is a subjective judgement, but recent published guidelines advise that the existence of the following should be considered:

- Automated decision-making
- Systematic monitoring of individuals (e.g. introducing CCTV)
- Processing sensitive data
- Processing personal data on a large scale (e.g. the implementation of a new HR IT system)
- Matching or combining datasets
- Processing data concerning vulnerable individuals
- Innovative use or application of technological or organisational solutions
- Data transfer across borders outside the European Union
- When the processing in itself "prevents data subjects from exercising a right or using a service or a contract".

The guidelines indicate that, as a very general rule of thumb, if the proposed change meets at least two of the above criteria, it should be considered high risk and therefore will require a DPIA.

An effective DPIA will be used throughout the development and implementation of a project, plan or proposal. It enables an organisation to systematically and thoroughly analyse how a particular change will affect the privacy of the individuals involved.

A DPIA can also be used to review the risks of an existing system, but the organisation needs to ensure that there is a realistic opportunity to implement necessary changes to mitigate the identified risks.

The purpose of the DPIA is to ensure that privacy risks are minimised while allowing the aims of the project to be met. These can be risks to the individuals affected, in terms of the potential for damage or distress. There will also be corporate risks to the organisation carrying out the project, such as the financial and reputational impact of a data breach.

Privacy risk is the risk of harm arising through an intrusion into privacy, through use or misuse of personal information. Some of the ways this risk can arise is through personal information being:

- Inaccurate, insufficient or out of date
- Excessive or irrelevant
- Kept for too long
- Disclosed to those who the person it is about does not want to have it
- Used in ways that are unacceptable to or unexpected by the person it is about
- Not kept securely.

Harm can present itself in different ways. Sometimes it will be tangible and quantifiable, for example financial loss or losing a job. At other times it will be less defined, for example damage to personal

relationships and social standing arising from disclosure of confidential or sensitive information. Sometimes harm might still be real even if it is not obvious, for example the fear of identity theft that comes from knowing that the security of information could be compromised.

The analysis in a DPIA should be checked by consulting with data subjects that are affected by the change. Consultation is an important part of a DPIA and allows people to highlight privacy risks and solutions based on their own area of interest or expertise. There is no set process for conducting a consultation, however:

- Internal consultation will usually be with a range of internal stakeholders to ensure that all relevant perspectives are taken into account
- External consultation provides the opportunity to get input from the people who will ultimately be affected by the project and to benefit from wider expertise.

Where there is any doubt about whether the risk- mitigating activities are sufficient to allow the proposed changes to go ahead, the ICO can also be consulted for approval of the risk assessment.

The G10 – AP C DPIA Tool has been developed to support the DPIA process. It consists of a quick set of initial screening questions, the answer to which determines whether the full DPIA analysis is required. Specialist privacy advice must be sought if required, in the use of DPIAs.

The GDPR Owner is responsible for ensuring the DPIA screening questions are undertaken for all relevant change activities. The Chief Executive Officer (CEO) will sign off completed DPIAs.

Security of Data

For a full description of Information Security controls, see Policy IT02 – Information Security. But some of the points are also summarised here:

- All Wilson James workers are responsible for ensuring that any personal data which Wilson James holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by Wilson James to receive that information and has entered into a confidentiality agreement
- All personal data should be accessible only to those who need to use it
- Personal data should be:
    - Kept in a locked filing cabinet (with the key secured)
    - Kept in a locked drawer (with the key secured)
    - If computerised, password protected
    - Stored on (removable) computer media which are encrypted
- Care must be taken to ensure that PC screens and terminals are not visible except to authorised Employees of Wilson James
- Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation
- Manual records that have reached their retention date are to be shredded and disposed of as ‘confidential waste’
- Hard drives of redundant PCs are to be removed and immediately destroyed before disposal.
- Processing of personal data ‘off-site’ presents a potentially greater risk of loss, theft or damage to personal data. Staff must be specifically authorised to process data off-site.

Disclosure of Data

Wilson James must ensure that personal data is not disclosed, either verbally or in writing, to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Wilson James workers should exercise caution when asked to disclose personal data held on

another individual to a third party. It is important to bear in mind whether disclosure of the information is relevant to, and necessary for, the conduct of Wilson James' business.

The GDPR permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:

- To safeguard national security
- Prevention or detection of crime including the apprehension or prosecution of offenders
- Assessment or collection of tax duty
- Discharge of regulatory functions (includes health, safety and welfare of persons at work)
- To prevent serious harm to a third party
- To protect the vital interests of the individual, this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the GDPR Owner.

Personal Data Breaches

Personal data breaches can take many forms. For example, unauthorised access, sending personal data to an incorrect address (postal or email), computing devices or paperwork containing personal data being lost or stolen. It is extremely important that all Wilson James workers (employees, contractors, agency staff) are able to recognise what constitutes a personal data breach, because under GDPR it is now mandatory to report them.

All personal data breaches must be reported internally to Wilson James using the email address: dataprotection@wilsonjames.co.uk. Under GDPR, where there is a risk to the rights and freedoms of data subjects, data breaches must also be reported to the supervisory authority within 72 hours of being discovered. If the breach is likely to result in a high risk to the rights and freedoms of individuals, the affected individuals must also be informed without undue delay. The GDPR Data Breach Procedure contains more detail about the requirement for data breach reporting.

Audit Procedure

Wilson James will be subject to an audit, every 6 to 12 months which can be internally or externally run, using the G10 – AP D Audit Tool. The audit scores will be reported to the Board of Directors and the GDPR Owner will be responsible for leading the actions resulting from the audit.

Appendix 1 – Glossary of Terms

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data subject – any living individual who is the subject of personal data held by an organisation.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Processor – a natural or legal person, public authority, agency or other body which processes personal data on behalf of a controller.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Supervisory Authority - an independent public authority which is established by a Member State. For the UK the Supervisory Authority is the Information Commissioner's Office (ICO)

Representative – a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation.

Consent – of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Recipient – a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data

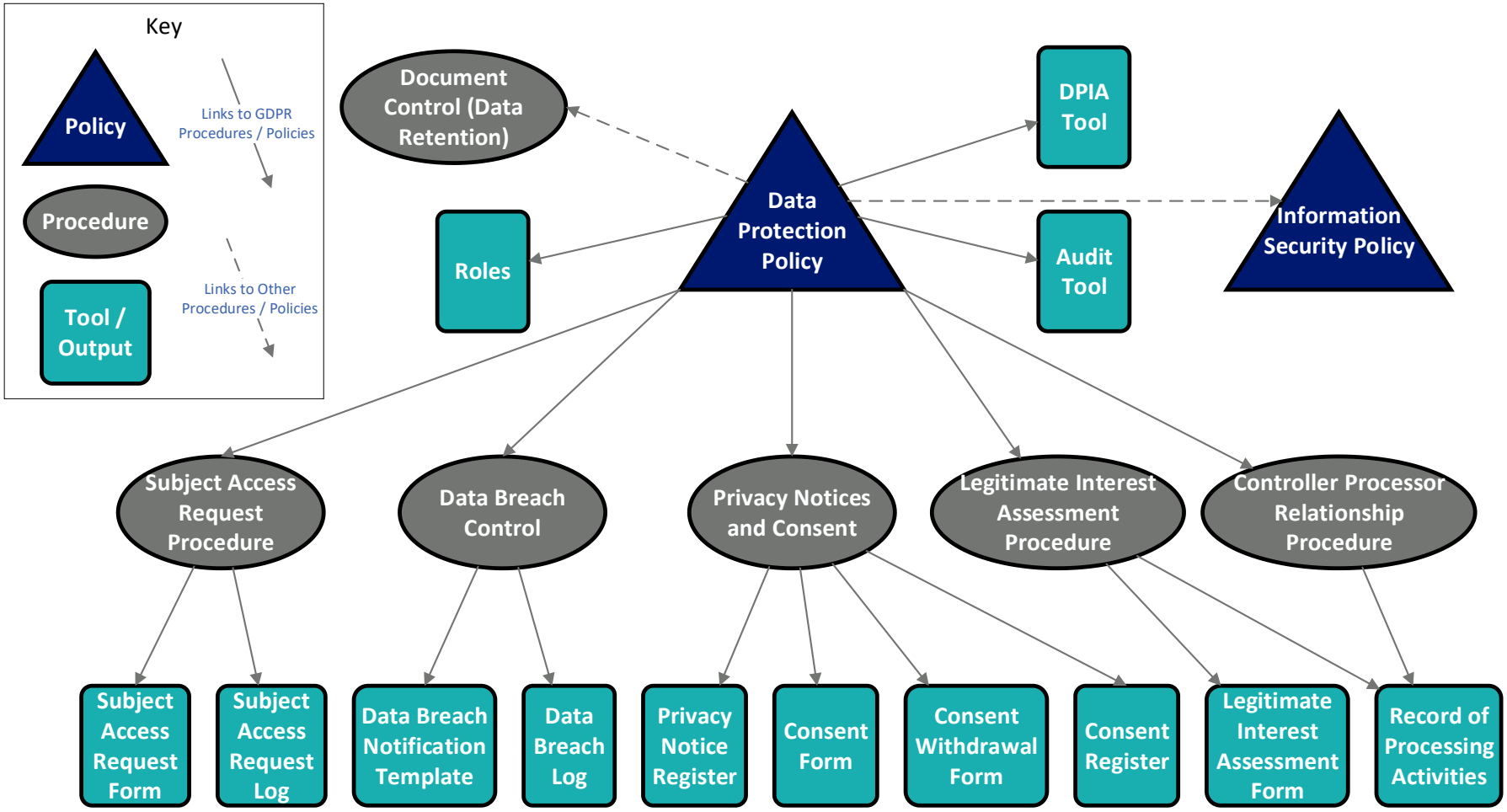
in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

Binding Corporate Rules - personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity

WILSON JAMES POLICY STATEMENT

Appendix 2

GDPR Policy Design:



WILSON JAMES POLICY STATEMENT

Appendix 3

The folder design and access model for GDPR related operational artefacts stored on the Z drive is as follows:

				Access Model				
Main Folder	**Folder**	**Sub Folders**	**Content**	**GDPR-O**	**DM**	**LM**	**Board**	**All**
GDPR	Policy Suite	Current	Policy and Procedures, Job descriptions	R/W	R/W	RO	RO	IMS
		Under Amendment	Policy and Procedures, Job descriptions	R/W	R/W	RO	N/A	N/A
	Subject Rights	Knowledge Base	SAR Tools, Form Templates and useful guides	R/W	R/W	RO	RO	N/A
		Log	SAR Log and performance reports	R/W	R/W	RO	N/A	N/A
		Audit Trail	Completed SAR forms and records of escalated decisions	R/W	R/W	RO	RO	N/A
	Data Breaches	Knowledge Base	Data Breach tools, form templates and useful guides	R/W	R/W	RO	RO	N/A
		Log	Data Breach Log and performance reports	R/W	R/W	RO	N/A	N/A
		Audit Trail	Completed Data Breach forms, Completed Notifications to ICO / Data Subjects	R/W	R/W	RO	RO	N/A
	Privacy and Consent	Knowledge Base	Consent form templates, Privacy Notices, useful guides	R/W	R/W	RO	RO	N/A
		Log	Consent register, Privacy Notice register	R/W	R/W	RO	N/A	N/A
		Audit Trail	Completed consent forms, old versions of Privacy Notices	R/W	R/W	RO	RO	N/A
	Analysis and Audit	DPIA	Template and completed DPIAs	R/W	R/W	R/W	RO	N/A
		Record of Processing	Record of processing activities catalogue, legitimate Interest assessments	R/W	R/W	R/W	RO	N/A
		Compliance Audits	Template and completed Compliance Audits	R/W	R/W	RO	RO	N/A
		Action Plans	Plans for tracking compliance activities and contractual reviews.	R/W	R/W	RO	RO	N/A
	Client Contractual Requirements	Data Clauses	Copies of data clauses that have been agreed with clients and suppliers	R/W	R/W	RO	RO	N/A

Roles for Access Model
GDPR-O Is the GDPR Owner role
DM is the Data Manager role
LM is the Line Manager role
Board is the Board of Directors and Heads of Department
All is all other Wilson James employees