EMPLOYEE DATA PROTECTION AND PRIVACY POLICY

Contents

Definitions

Personal data means any information relating to an individual 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;

Processing means any operation or set of operations which is performed on personal data or on a set 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;

Data includes information in any form which can be processed including automated, electronic and manually created data.

Automated data is information created or held online such as that held on the computer or online in the HR Management system HR Duo.

Manual data means information that is kept as part of a relevant filing system or with the intention that it should form part of a relevant filing system. Examples of these are traditional paper files, reports and statements as well as personnel and financial records which are used as part of our daily operational duties. Personal data means data relating to a natural and legal person.

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of processing of personal data; where the purposes and means of such processing are determined by the Regulation or Data Protection legislation, the controller or the specific criteria for examination may be provided for by union or member state law;

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; For example, HR Duo is a processor of HR data for the organisation.

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subjects wishes by which he or she by statement or by a clear informative action signifies agreement to the processing of personal data related to him or her.

In the context of an employment relationship consent for the processing of data is given in the employment contract or is set out in the various pieces of employment legislation which guide and direct the management of data within the employment relationship.

Sensitive personal data relates to specific categories of data which are identified as data relating to persons racial origin, political opinions, religious or other beliefs, physical or mental health, sexual life, criminal convictions or the alleged commission of an offence, membership of the trade union.

Examples of these types of data are files which contain details of allegations, prosecutions or convictions with regard to an individual.

1. Introduction

General Data Protection Regulation (GDPR) concerns the personal data of staff members wherever that data is held, the management of that data in the way specified in the regulation and processes for dealing with data protection breaches.

The purpose of this policy is to provide you with clear information on the way we process and use personal data in accordance with the requirements of the Regulation.

2. Scope

This policy applies to all employees.

You are entitled to: -

1. Establish the existence of personal data kept in relation to you - this includes being informed of what data will be collected, why, by whom, for what purpose and where the data will go;
2. To have access to the data (with some exceptions, e.g. where a personal opinion is expressed and it is known to be in confidence (interview notes etc.);
3. To have inaccurate data rectified, blocked or erased.
4. To have the data removed when no longer necessary to have data erased, to restrict processing, the right to object (please note employment context below).

Please note that in an employment context information in the form of data is essential for us in fulfilling our duties as an employer. This means that where the personal data collected and processed is required to fulfil a contract of employment with you, explicit consent is not required. This will often be the case where the contract cannot be completed without personal data in question.

Secondly if personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required - this may be the case for some data related to employment and taxation for example and for many areas addressed by the public sector. Typically, this will relate to recording working hours, annual leave et cetera.

The above limits your ability to have data removed, erased, restrict processing or to object.

3. Policy Statement

As your employer, we need to keep and process information about you for normal employment purposes. The information we hold and process will be used for our management and administrative use only. We will keep and use it to enable us to run the business and manage our relationship with you effectively, lawfully and appropriately, during the recruitment process, whilst you are working for us, at the time when your employment ends and after you have left.

This includes using information to enable us to comply with the employment contract, to comply with any legal requirements, pursue the legitimate interests of the Organisation and protect our legal position in the event of legal proceedings. If you do not provide this data, we may be unable in some circumstances to comply with our obligations and we will tell you about the implications of that decision.

We may sometimes need to process your data to pursue our legitimate business interests, for example to prevent fraud, administrative purposes or reporting potential crimes.

Much of the information we hold will have been provided by you, but some may come from other internal sources, such as your manager, or in some cases, external sources, such as referees and Revenue.

The sort of information we hold includes your application form and references, your contract of employment and any amendments to it; correspondence with or about you, for example letters to you about increments or, at your request, a letter to your mortgage company confirming your salary; information needed for payroll, benefits and expenses purposes; contact and emergency contact details; record of working hours, annual leave, sickness and other absences; information needed for equal opportunities monitoring policy; and records relating to your career history, such as training records, performance management appraisals and, where appropriate, disciplinary and grievance records.

You may, inevitably be referred to in many Organisation documents and records that are produced by you and your colleagues in the course of carrying out your duties and the business of the Organisation.

In the course of its business, we may take photographs for a number of reasons. These include staff photographs or event photographs which may be used in publications, on the corporate website or corporate twitter account. An employee can opt out of this at any stage, and request this in writing to HR.

Where necessary, we may keep information relating to your health, which could include reasons for absence and GP reports and notes. This information will be used in order to comply with our health and safety and occupational health obligations – to consider how your health affects your ability to do your job and whether any adjustments to your job might be appropriate. We will also need this data to administer and manage statutory and Organisation sick pay.

Where we process special categories of information relating to your racial or ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, biometric data or sexual orientation, we will always obtain your explicit consent to those activities unless this is not required by law or the information is required to protect your health in an emergency.

Where we are processing data based on your consent, you have the right to withdraw that consent at any time.

We have the authority and ability to monitor emails, internet usage, network and PC activity, as detailed in our Staff handbook, available on the intranet (if applicable) and online on HR Duo.

Other than as mentioned below, we will only disclose information about you to third parties if we are legally obliged to do so or where we need to comply with our contractual duties to you, for instance we may need to pass on certain information in the event that the payroll function is outsourced or for pension or health insurance schemes.

We may transfer information about you to other state organisations or government departments for purposes connected with your employment and pension.

If in the future, we intend to process your personal data for a purpose other than that which it was collected, we will provide you with information on that purpose and any other relevant information.

In Summary

1. During your employment and for as long as necessary after your employment we will hold, use and process your personal data for the purposes of staff administration, management, and the legal or business needs of the employment.
2. Examples of personal data include but are not limited to: employment records and related information such as absence/attendance, injury or sickness details, disciplinary/or performance records, full name, address, membership of a trade union, information on an offence committed etc.
3. We undertake not to ask our employees or prospective employees to make a data access request seeking personal data from other sources for the purpose of making it available to us.

If any of the data held about you is inaccurate you have a right to have it corrected or annotated. You should contact your line manager in this regard.

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the Regulation (Appendix 4).

After the required retention schedule has expired we undertake to carry out the destruction of the data in a secure manner (see Appendix 1 for retention schedule).

4. Subject Access Request

Subject Access Request	**Timeline**
The right to be informed	When data is collected (if supplied by data subject) or within one month (if not supplied by data subjects)
The right of access	One month
The right of rectification	One month
The right to erasure	Without undue delay and providing it does not breach any contractual or legislative requirements to retain the employee information
The right to restrict processing	Without undue delay and providing it does not breach any contractual or legislative requirements to retain the employee information
The right to data portability	One month providing it does not breach any contractual or legislative requirements to retain the employee information
The right to object	On receipt of objection

Rights in relation to automated decision making and profiling	Not specified

Obligations and Rights of Managers and Staff Members

Under the General Data Protection Regulation (GDPR) and The Data Protection Act 2018 (DPA) you have a number of rights with regard to your personal data. You have the right to request from us access to and rectification or erasure of your personal data, the right to restrict processing, object to processing as well as in certain circumstances the right to data portability.

If you have provided consent for the processing of your data you have the right (in certain circumstances) to withdraw that consent at any time which will not affect the lawfulness of the processing before your consent was withdrawn.

You have the right to lodge a complaint to the Data Protection Commissioner if you believe that we have not complied with the requirements of the GDPR or DPA 18 with regard to your personal data.

- You are expected to comply with the Data Protection Regulation and assist us to comply with our obligations under the Data Protection legislation when dealing with personal data of any kind.
- You must only access, change, erase, copy, or make use of any information (including personal data) if you are authorised to do so and if it is in keeping with your allocated work duties.
- You must not pass on personal data about any individual where those details are known to you because of your employment with the organisation, unless you have the prior consent of the individual.
- You are responsible for informing us of any changes in your personal details e.g. change of address etc.
- You are entitled to be given a description of any data held about you and the purposes for which it is kept, and we undertake to provide this information to you within 21 days of the date of request.
- You are entitled to request any personal data held about you by the organisation, through a “Subject Access Request” and we undertake to provide this data within 30 days of receiving such request. It may be necessary to disclose such information to third parties, but we will only do so when it is strictly necessary.
- Failure to abide by this policy may result in disciplinary action

Data Controller

The Employer is the Data Controller for this employment being the body who controls the collection and processing of personal information. The Managing Director/CEO is the individual within the employment who has responsibility for Data Protection. The Company will appoint a Data Processing Coordinator to manage Data Protection on a day-to-day basis including data protection requests.

The Data Controller is responsible for the following: -

- Keeping personal data up to date as required.
- Retaining personal data no longer than necessary.
- Day to day security of the office environment (manual and automated records).
- Methods of handling personal information are clearly described and documented.
- All staff handling personal information are appropriately trained to do so.

- All staff handling personal information are appropriately supervised.
- Performance with handling personal information is regularly assessed and reviewed.
- The Data Protection administrator is kept informed of manual and automated systems storing and/or processing personal information.
- Continuous assessment of the need for all current personal information storage and processing and elimination of any that is not necessary.

A Data Processor is a person who processes personal information on behalf of the data controller. Processing means performing any operation or set of operations on data including:

- Obtaining, recording or keeping data
- Collecting, organising, storing, altering or adapting data
- Retrieving, consulting or using data
- Disclosing the data by transmitting, disseminating or otherwise making available
- Aligning, combining, blocking, raising or destroying data

Where we use 3rd parties to process information on our behalf we will have a contract containing the relevant Data Protection clauses to ensure that the 3rd party only processes personal data in accordance with our instructions and that the same standards of security are adhered to. In addition, we may be obliged to disclose personal information relating to individuals to 3rd parties to comply with legal requirements, as well as to protect and defend the rights of property of the employment.

Contracts Involving the Processing of Personal Data
We will ensure that all relationships we enter into that involve the processing of personal data are subject to a documented contract that includes the specific information and terms required by the GDPR.

HR Duo HR Limited
HR Duo HR Ltd is a data processor who processes personal information on behalf of the Data Controller. This information is managed under specified conditions in their HR Services Offices.

Where the information is stored online on HR Duo, it is served over a secure HTTPS connection between users and our web servers. HR Duo data is stored in AWS's Ireland Data Centres and is accessible only to HR Duo's CTO, using an encrypted connection. No information is passed to countries outside the EEA.

Within its Apps, HR Duo has implemented authentication and authorisation to ensure that user information is only exposed to relevant HR Duo managers and its HR Administrators whether in HR Duo HR Services Office or in this organisation.

Within the HR Duo HR Services Office, the information is only accessible by staff identified to us who have signed confidentiality agreements and who are fully aware to the requirements of the contract signed between HR Duo and the organisation relating to data protection.

HR Duo HR Limited and the Company have signed a Data Protection Contract which is specifically compliant with the requirements of the Regulation in respect of third party processing as set out

above.

Data Protection Officer
A defined role of Data Protection Officer is required under the GDPR for public authorities, organisations that perform large-scale monitoring or which process particularly sensitive types of data on a large-scale.

The Company will appoint an employee to manage the requirements of data protection standards and agreements as a Data Protection Officer.

Privacy by Design
We have adopted the principle of Privacy by Design and will ensure that the definition and planning of all new or significant change systems that collect, and process personal data will be subject to due consideration of privacy issues including the completion of one or more Data Protection impact assessments.

Privacy by Default
We have adopted the principle of Privacy by Default and will ensure that security settings are automatically protective of Privacy of Data Subjects.

Data Breach Notification
Information/data is one of our most important assets and each one of us has a responsibility to ensure the security of this information.

Accurate, timely, relevant and properly protected information/data is essential to the successful operation of the Employment. Sometimes a breach of information/data security may occur because this information/data is accidentally disclosed to unauthorised persons or, lost due to a fire or flood or, stolen as result of a targeted attack or the theft of a mobile computer device. The following are examples: –

- The disclosure of confidential data to unauthorised individuals;
- Improper disposal of documents leaving personal data deposited in a bin that can be accessed by the general public;
- Loss or theft of data or equipment on which data is kept;
- Loss or theft of paper records;
- Inappropriate access controls allowing unauthorised use of information;
- Suspected breach of the Employment's security and related policies;
- Attempts to gain unauthorised access to computer systems, e.g. hacking;
- Viruses or other security attacks on employment's IT equipment systems or networks;
- Breaches of physical security;
- Confidential information left unlocked in accessible areas; and
- Emails containing personal or sensitive information sent in error to the wrong recipient.

In line with the Regulation, where breaches known to have occurred which are likely to result in a risk to the rights and freedoms of individuals, the relevant supervisory authority will be informed within 72 hours. This will be managed in accordance with our Management Guidelines for Dealing with Data Breaches which is attached as Appendix 2.

All information/data breaches must be reported to the Data Controller immediately. Members of staff and their line manager must do this verbally and in writing for breaches involving manual (paper based) information/data or for breaches involving electronic data. Any third-party processors have through contract, the same obligation.

Addressing Compliance with the Regulation

The following actions are undertaken to ensure that we comply at all times with the accountability principle of the GDPR: –

- The legal basis for processing personal data is clear and unambiguous
- Staff have been appointed with specific responsibility for data protection in the organisation
- All staff involved in handling personal data understand their responsibilities for following good data protection practice
- Briefing in data protection has been provided to all staff
- Rules regarding consent are followed
- Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
- Regular reviews of procedures involving data protection are carried out
- Privacy by design is adopted for all new or changed systems and processes
- The following documentation of processing activities is recorded:

    - Organisation name and relevant details
    - Purposes of the personal data processing
    - Categories of individuals and personal data processed
    - Categories of personal data recipients
    - Agreements and mechanisms for transfer of personal data to non-EU countries including details of controls in place
    - Personal data retention schedules
    - Relevant technical and organisational controls in place
    - These actions are reviewed on a regular basis as part of the management process concerned with data protection.

5. Appendix 1 - HR Retention Periods

Notes

1. ***Reference to HR refers to the person responsible for HR internally in the organisation***
2. ***Third party provider refers to HR, payroll and benefits as appropriate***
3. ***Not all HR retention periods apply within this organisation but where it does we apply the retention periods set out here***

Recruitment Data

Data Type	Why is it Collected	Who can access	Security	GDPR Reason	Retention Limit
Application Form/ Letter of Application	Establish suitability for the position.	HR Shortlisting Manager Interviewing Manager	Stored in Lockable Filing Cabinet. HR/ Relevant Manager (if appropriate) own access to files. If stored online: access will be protected through limitations on access and online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent.	If successful – term of employment and 7 years post termination. If unsuccessful - 18 months after closing of vacancy. Unsolicited application - 12 months from receipt.
CV	To establish suitability for post.	HR Shortlisting Manager Interviewing Manager	Stored in Lockable Filing Cabinet. HR/ relevant manager (if appropriate) own access to files. If stored online: access will be protected through limitations on access and online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent.	If successful – term of employment and 7 years post termination. If unsuccessful - 18 months after closing of vacancy. Unsolicited application - 12 months from receipt
Health Questionnaire	To establish suitability for the	HR Line Manager	Stored in Lockable Filing Cabinet. HR/ relevant manager own access to files.	Consent.	If successful – term of employment and 7 years

	role		If stored online: access will be protected through limitations on access and online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server storage data Company Doctor		post termination. If unsuccessful - 18 months after closing of vacancy.
Aptitude Testing	To establish suitability for post	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server storage data Aptitude Testing Company	Consent.	If successful – term of employment and 7 years post termination. If unsuccessful - 18 months after closing of vacancy.
Interview Questions and notes from Interview	To record questions asked and responses to ensure compliance with Equality Act and establish suitability for post.	HR Interviewing Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent.	If successful – term of employment and 7 years post termination. If unsuccessful - 18 months after closing of vacancy.
Interview Scoring Sheets	To attribute a score to establish suitability for post.	HR Interviewing Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and	Consent.	If successful – term of employment and 7 years post termination.

			online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server storage data		If unsuccessful - 18 months after closing of vacancy.
Offer Letters	To record contractually what was offered/committed to the candidate.	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent.	If successful – term of employment and 7 years post termination. If unsuccessful - 18 months after closing of vacancy.
Rejection Letters	To record reason for rejection.	HR	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent.	6 months after rejection.
Recruitment Consent Form	To establish consent to process data/store data.	HR Data Controller	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security measures. Third Party Provider to store either in lockable filing cabinets or password protected server	Consent.	If successful – term of employment and 7 years post termination. If unsuccessful - 18 months after closing of vacancy.

			storage data		

Payroll Information

Data Type	Why is it collected	Who can access	Security	GDPR Reason	Retention Limit
Payroll Records	To enable pay to be processed and payments to be made.	Data processor – payroll HR Line Manager Finance Manager ROS	Stored in Lockable Filing Cabinet - Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Tax and Social Insurance History	To be held for Revenue Requirements	HR Data Processor – Payroll Line Manager Finance Manager ROS	Stored in Lockable Filing Cabinet - Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Tax Credits	To enable pay to be processed and	HR Data Processor –	Stored in Lockable Filing Cabinet - Finance own access to files.	Legal	Term of employment and 7 years post termination.

	payments to be made.	Payroll Line Manager Finance Manager ROS	If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data		
P45	To enable pay to be processed and payments to be made	HR Data Processor - Payroll Line Manager Finance Manager ROS	Stored in Lockable Filing Cabinet - Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
P60	To enable pay to be processed and payments to be made and Revenue Requirements.	HR Data Processor – Payroll Line Manager Finance Manager ROS	Stored in Lockable Filing Cabinet - Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Court Instructions	To enable pay to be processed and payments to be made and benefits agencies requirements.	HR Data Processor – Payroll Finance Manager ROS	Stored in Lockable Filing Cabinet - Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.

Salary Sacrifice Data	To be held for Revenue requirements	HR Data Processor – Payroll Line Manager Finance Manager ROS	Stored in Lockable Filing Cabinet - Finance own access to files. Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.

Personnel File

Data Type	**Why is it Collected**	**Who Can Access**	**Security**	**GDPR Reason**	**Retention Limit**
Offer Letters	To record contractually what was offered/committed to the candidate.	Line Manager HR Data Processor - Payroll	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Copy of Passport (or other right to work data)	To establish eligibility to work in Ireland.	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server	Legal	Term of employment and 7 years post termination.

			storage data		
Health Questionnaire recruitment information	To establish if they are medically capable of carrying out the job that has been offered.	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent.	Term of employment and 7 years post termination.
Job Description	To record detail of the job that they are currently undertaking	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Retain Indefinitely
Garda Vetting	To establish if criminal record. To establish that they are suitable for the job and do not pose a risk to children or vulnerable adults.	HR	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal or Consent	Term of employment and 7 years post termination.
References	Establish their suitability for the job on consent of employee.	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security	Legal or Consent	Term of employment and 7 years post termination.

			Third Party Provider to store either in lockable filing cabinets or password protected server storage data		
Contract of Employment	Record their contractual terms of employment.	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Other Contractual Letters	Record their agreed variations to their contractual terms.	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Flexible Working Requests	Record any flex working requests and any agreed changes and/or rejected changes to their contractual terms.	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Restrictive Covenants	To record any restrictive contractual terms	HR Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through	Legal	Term of employment and 7 years post termination (in case there is a breach

	that will survive post termination.		limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data		found later).
Confidentiality Letters	To record any data confidentiality contractual terms that will survive post termination.	HR Data Controller Line Manager	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination (in case there is a breach found later).
Data Consent Forms	To obtain consent for processing of personal data.	HR Line Manager Data Controller – Payroll	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Pay Scales Data Pay point	To record their actual pay and reasons for allocating them a pay point/position on a salary scale.	HR Line Manager Data Controller – Payroll	Stored in Lockable Filing Cabinet. HR/Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.

Personal Data

Data Type	Why is it Collected?	Who can Access?	Security	GDPR Reason	Retention Limit
Name	To uniquely identify the employee	HR Line Manager ROS/ Revenue	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Address	To be able to identify the employee and send correspondence to employee	HR Line Manager Data Controller – Payroll ROS/ Revenue	Stored in Lockable Filing Cabinet. HR/Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent	Term of employment and 7 years post termination.
PPS Number	To uniquely identify employee for government/revenue purposes.	HR Line Manager Data Processor - payroll Finance Manager ROS/ Revenue	Stored in Lockable Filing Cabinet. HR/Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post termination.
Date of Birth	Know their age for NMW purposes,	Line Manager	Stored in Lockable Filing Cabinet. HR/Finance	Legal	Term of employment and

	redundancy calculations, Driving Licence and other age-related qualifications, OWT rest break requirements, and pension purposes.	HR Data Processor - payroll	own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data		7 years post termination.
Details of Next of Kin	Make contact in emergencies	Line Manager HR	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent Or Vital Interest	Upon Leaving
Exit Interview	Record details of termination date and close all necessary systems/benefit agreements.	Line Manager HR	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent	7 Years post-termination

Employment History and Qualifications

Data Type	Why is it Collected?	Who can Access?	Security	GDPR Reason	Retention Limit
Summary of post held in the organisation.	Record their history of positions held within the company.	HR Line Manager Data Processor - payroll	Stored in Lockable Filing Cabinet. HR/Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent	Term of employment and 7 years post-termination.

Young persons in employment

Data Type	Why is it Collected?	Who can Access?	Security	GDPR Reason	Retention Limit
Qualifications Certificate	Adhere to National Minimum Age whilst employed within the company.	HR Line Manager Health & Safety Officer	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server	Consent Or Legal	3 years

			storage data		

Performance and Development

Data Type	**Why is it Collected?**	**Who can Access?**	**Security**	**GDPR Reason**	**Retention Limit**
Record of Training Courses Attended and Expiry Dates	Record dates of training courses attended and when training is required to be re-assessed	HR Line Manager Health & Safety Officer	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal Or Consent	Course feedback -1 Year. Completion of training - 7 years.
Any Performance Discussions	Record any performance discussion held and improvement requests made.	Line Manager HR Investigative Officer	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server	Legal	Term of employment and 7 years post-termination.

			storage data		
Performance scoring / rating documents	Record any performance rating data that may influence pay decisions.	HR Line Manager Investigative Officer	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Term of employment and 7 years post-termination.

Discipline and Grievance

Data Type	**Why is it Collected**	**Who can Access**	**Security**	**GDPR Reason**	**Retention Limit**
Disciplinary warnings issued	Record any disciplinary/capability warnings issued and a summary of future behaviour expectations.	HR Line Manager Investigative Officer	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Letter to be removed from personnel file after the prescribed period.
Disciplinary investigations	Make a record of any investigations that have been carried out in relation to his employee.	HR Line Manager Investigative Officer	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security	Legal	Letter to be removed from personnel file after the prescribed period.

Grievances Raised	Record any grievances or grievance investigations that have been carried out in relation to this employee (or raised by this employee and a record of any agreed outcomes.	HR Line Manager Investigative Officer	Stored in Lockable Filing Cabinet. HR own access to files. If stored online: access will be protected through limitations on access and online security	Legal	Letter to be removed from personnel file after the prescribed period.

Health and Wellbeing

Data Type	**Why is it Collected**	**Who can Access**	**Security**	**GDPR Reason**	**Retention Limit**
Absence Data	Record number of days absences to allow for absence policy monitoring/trigger points to be compiled with.	HR Line Manager Data Processor– Payroll Company Medical Staff	Stored in Lockable Filing Cabinet. HR/Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Non-work-related illness – 3 years. Work-related Illness - Term of employment and 7 years post-termination.
Medical Reports	Enable the Company to fully understand a medical condition and to know what adjustments might be made in the	HR Line Manager 3rd Party Benefit Provider Company Medical	Stored in Lockable Filing Cabinet. HR/Finance own access to files. If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server	Legal	Non-work-related illness – 3 years. Work-related Illness - Term of employment and 7 years post-termination.

	workplace.	Staff	storage data		
Health Questionnaire	To enable the Company to fully understand a medical condition and to know what adjustments might be made in the workplace.	Company Medical staff HR Line manager	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Non-work-related illness – 3 years. Work-related Illness - Term of employment and 7 years post-termination.
Medical Certificates	To record the reasons for absence and to allow SSP and/or Co sick pay to be paid under the sick pay policy	Company Medical staff HR Line manager Data processor - payroll	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Non-work-related illness – 3 years. Work-related Illness - Term of employment and 7 years post-termination.
Medical Benefit Records	To enable enrolment in the private medical benefit	Company Medical Staff HR 3rd party benefit provider	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	Non-work-related illness – 3 years. Work-related Illness - Term of employment and 7 years post-termination.

Working Time

Data Type	**Why is it Collected**	**Who can Access**	**Security**	**GDPR Reason**	**Retention Limit**

Working Time recording data	To ensure compliance with Working Time Legislation time recording requirements	HR Line manager Data processor - payroll Investigative Officer	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	3 years
Time and Attendance Data	To ensure compliance with Working Time Legislation time recording requirements	HR Line manager Data processor - payroll Investigative Officer	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	9 months after date of leaving
Annual Leave	To ensure compliance with Working Time Legislation requirements	HR Line manager Data processor - payroll Investigative Officer	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	3 years
Public Holidays	To ensure compliance with Working Time legislation requirements	HR Line manager Data processor - payroll	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server	Legal	3 years

			storage data		
Night Workers Health Questionnaire	To ensure compliance with Working Time Legislation time recording requirements for night workers	Company Medical staff HR Line manager Investigative Officer	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	3 years

Protected Leave

Data Type	**Why is it Collected**	**Who can Access**	**Security**	**GDPR Reason**	**Retention Limit**
Carers Leave	To ensure compliance with Department of Social Protection Requirements requirements.	HR Line manager Data processor - payroll	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	8 years
Maternity Leave	To ensure compliance with Department of Social Protection Requirements.	HR Line manager Data processor - payroll	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	7 years

Adoptive Leave	To ensure compliance with Department of Social Protection Requirements.	HR Line manager Data processor - payroll	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	7 years
Parental Leave	To ensure compliance with Department of Social Protection Requirements.	HR Line manager Data processor - payroll	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	12 years
Force Majeure	To ensure compliance with Policy document.	HR Line manager Data processor - payroll	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	8 years

Travel and Expenses

Data Type	**Why is it Collected**	**Who can Access**	**Security**	**GDPR Reason**	**Retention Limit**
Travel Expenses	To ensure adherence	Finance Manager	If stored online: access will be protected through	Legal	7 Years post-termination

submitted	to the Travel expense policy	Data processor– payroll HR Line manager Investigative Officer	limitations on access and online security Stored in lockable filing cabinet - Finance own access to files Third Party Provider to store either in lockable filing cabinets or password protected server storage data		after which, anonymised

Vehicle Tracking

Data Type	**Why is it Collected**	**Who can Access**	**Security**	**GDPR Reason**	**Retention Limit**
Vehicle Tracking Information	To enable reimbursement of proper expenses To ensure adherence to the Travel expense policy	Finance Manager Data processor– payroll HR Line manager Investigative Officer	If stored online: access will be protected through limitations on access and online security Stored in lockable filing cabinet - Finance own access to files	Legal	3 Years

Employee Surveys

Data Type	**Why is it Collected**	**Who can Access**	**Security**	**GDPR Reason**	**Retention Limit**
Data of Their Submissions	To record their comments, suggestions about the company To enable rewards under the staff survey and	HR Line manager	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security	Legal Or Consent	2 years

	participation policies				

Future References

Data Type	Why is it Collected	Who can Access	Security	GDPR Reason	Retention Limit
Copy of references sent to prospective /exiting employees	To maintain a record of what has been sent in response to a reference request to ensure compliance with false representation legislation.	HR Line manager	Stored in lockable filing cabinet - HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	1 Year after issue

Information Sent to Third Parties

Data Type	Why is it Collected	Who can Access	Security	GDPR Reason	Retention Limit
Pensions	To enable participation in the pension scheme	HR Data processor - payroll Finance Manager 3rd party benefit provider	Stored in lockable filing cabinet - Finance and HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal or Consent	Indefinite
Medical Benefits	To enable	Company Medical	Stored in lockable filing cabinet	Legal	12 months after the data

	participation in the private medical scheme	Staff Data Processor – Payroll HR 3rd Party benefit provider	Finance and HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data		was provided to the Third Party Provider
EAP	To enable participation in the employee assistance programme/ helpline scheme	Company Medical staff HR Line Manager	Stored in lockable filing cabinet - Finance and HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Consent	12 months after the data was provided to the Third Party Provider
Rail Ticket	To enable participation in the Rail Ticket scheme	HR Data processor – payroll Finance Manager Line manager	Stored in lockable filing cabinet - Finance and HR own access to files If stored online: access will be protected through limitations on access and online security Third Party Provider to store either in lockable filing cabinets or password protected server storage data	Legal	12 months after the scheme has competed
Bike to Work Scheme	To enable participation in the bike to work scheme	HR Data processor – payroll Finance Manager	Stored in lockable filing cabinet - Finance and HR own access to files If stored online: access will be protected through limitations on access and online security	Legal	12 months after the scheme has competed and the bike is transferred to the employee

		Line manager	Third Party Provider to store either in lockable filing cabinets or password protected server storage data		

6. Appendix 2 - Data Breach Guidelines

1. It is a requirement of the EU General Data Protection Regulation 2016 (GDPR) that incidents affecting personal data that are likely to result in a risk to the rights and freedoms of data subjects must be reported to the data protection supervisor authority, without undue delay and where feasible, within 72 hours of becoming aware of it. In the event that the 72-hour target is not met reasons for the delay must be given.

2. Where the incident affects personal data, a decision must be taken regarding the extent, timing and content of communication with data subjects. The GDPR requires that communication must happen "without undue delay" if the breach is likely to result in the "high risk to the rights and freedoms of natural persons". The exact nature of an incident and its impact cannot be predicted with any degree of certainty and so it is important that a risk based approach be undertaken when deciding what to do. It is not a foregone conclusion that the breach must be notified to either supervisory authority or the data subjects affected. However, there must be an assessment of the risk that the breach represents to the "the rights and freedoms of natural persons" (GDPR article 33").

3. The GDPR states that a personal data breach shall be notified to the supervisory authority "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons" (GDPR article 33). This requires the employer to assess the level of risk before deciding whether or not to notify. If you are unsure it would be prudent to notify.

4. Factors to take into account as part of this risk assessment should include: –
    a. Whether the personal data was corrupted
    b. If encrypted, the strength of the encryption used
    c. To what extent the data was pseudonymised (I.e. whether living individuals can reasonably be identified from the data)
    d. The data items included e.g. name, address, bank details, biometrics
    e. The number of data subject records involved
    f. The number of data subjects affected
    g. The nature of the breach e.g. theft, accidental destruction
    h. Any other factors that are deemed to be relevant
5. The parties involved in the risk assessments may include representatives from the following areas, depending on the nature and circumstances of the personal data breach
    a. Senior management
    b. Business areas
    c. Technology
    d. Information security
    e. Legal
    f. Data protection personnel
6. The risk assessment method, its reasoning and its conclusion should be fully documented and signed off by top management. The result of the risk assessment should include one of the following conclusions: –
    a. The personal data breach does not require notification. You must document why you came to this conclusion.
    b. The personal data breach requires notification to the supervisory authority only

c. The personal data breach requires notification both to the supervisory authority and to the affected data subjects

7. These conclusions may be subject to change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.
8. If it is decided to notify the supervisory authority, the GDPR requires that this be done "without undue delay and, where feasible, not less than 72 hours after having become aware of it" (GDPR article 33). If there are legitimate reasons for not having given the notification within the required timescale, these reasons must be given as part of the notification.
9. The following information must be given as part of the notification: –
    a. The nature of the personal data breach, including, where possible: –
        i. Categories and approximate number of data subjects concerned
        ii. Categories an approximate number of personal data records concerned
    b. Name and contact details of the data protection and in contact point where more information may be obtained
    c. A description of the likely consequences of the personal data breach
    d. Description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate its possible adverse effects
    e. If the notification falls outside the 72-hour window, the reasons why it was not submitted earlier
10. Written confirmation should be obtained from the supervisory authority of the personal data breach notification has been received, including the date and time at which it was received. Where necessary, the GDPR allows the information to be provided in phases without undue further delay
11. Documentation of the personal data breach, including its effect and the remedial action taken, will be produced as part of the Information Security Incident Response Procedure
12. The GDPR states that personal data breach shall be notified to the data subject "when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons" (GDPR article 34). Note the addition of the word "high" over and above the definition given in article 33.
13. The risk assessment carried out earlier in this procedure will have determined whether the risk to the rights and freedoms of the data subjects affected is judged to be sufficiently high to justify notification to them.
14. However, if measures have subsequently been taken to mitigate the high risk to the data subjects, so that it is no longer likely to happen, then communication to the data subjects is not required by the GDPR
15. Notification to affected data subjects is also not mandated by the GDPR where it "would involve a disproportionate effort" (GDPR article 34). However, in this case a form of public communication should be used instead.
16. This may change based on feedback from the supervisory authority and further information that is discovered as part of the ongoing investigation of the breach.
17. Once it has been decided that the breach justifies communication to the data subjects affected, the GDPR requires this be done without undue delay.
18. The communication to the affected data subjects "shall describe in clear and plain language the nature of the personal data breach" (GDPR article 34) and must also cover
    a. Name and contact details of the data protection contact person where more information may be obtained
    b. A description of the likely consequences of the personal data breach

c. Description of the measures taken or proposed to be taken to address the personal data breach including, where appropriate, measures to mitigate the possible adverse effects

19. In addition to the points required by the GDP or, it may be appropriate to offer advice to the data subject regarding actions they may be able to take to reduce the risks associated with the personal data breach.
20. In most cases it will be appropriate to notify affected data subjects via letter or email or both in order to ensure that the message has been received and that they have an opportunity to take the action required.

7. Appendix 3 - Subject Access Request Procedure

This procedure is intended to be used for the data subject exercises one or more of the rights they are granted under the European Union General Data Protection Regulation (GDPR).

Each of the rights involved has its own specific aspects and challenges to the employment in complying with them and doing so, within the required timescales. In general, a proactive approach will be taken which places as much control over personal data in the hands of the data subject as possible, with a minimum amount of intervention or involvement required on the part of the employment. This may be achieved by providing online access to personal data so that the data subject can verify and amended as required.

However, in some cases there is a decision-making process to be followed by the organisation regarding whether a request will be allowed are not; where this is the case the steps involved in these decisions are explained in this procedure.

Subject Access Request Procedure
The following general points applied to all of the requests described in this document and are based on article 12 of the GDPR: –

1. Information shall be provided to the data subject in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.
2. Information may be provided in writing, or electronically readable format, or by other means as required by data subject.
3. The data subject may request the information orally (e.g. over the telephone or face-to-face), as long as the identity of the data subject has been established.
4. We must act on a request from a data subject unless we are unable to establish their identity.
5. We must provide information without undue delay and within a maximum of one month from the receipt of the request.
6. The response timescale may be extended by up to 2 further months for complex or a high volume of requests – the data subject must be informed of this within one month of the request, and the reasons for the delay given.
7. If a request is made via electronic form, the response should be viewed via electronic means, where possible, unless the data subject requests otherwise.
8. If it is decided that we will not comply with a request, we must inform the data subject without delay and at the latest within a month stating the reason(s) and informing the data subject of their right to complain to the supervisory authority.
9. Generally, responses to requests will be made free of charge, unless they are “manifestly unfounded or excessive” (GDPR article 12), in which case we will either charge a reasonable fee or refuse to action the request.
10. If there is a doubt about a data subject’s identity, we will request further information to establish it.

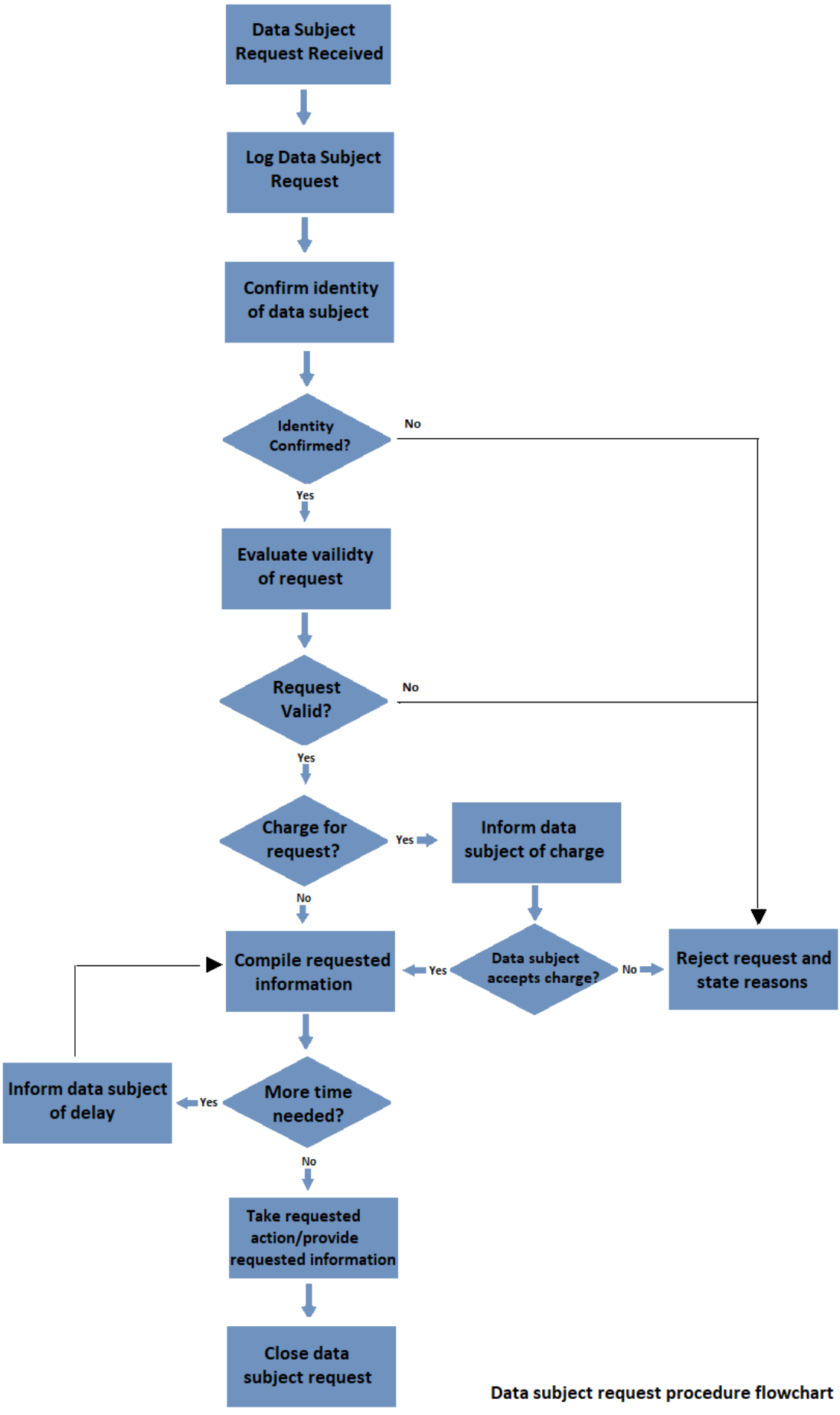
Please refer to the exact text of the GDPR if clarification of any of the above is required.

The procedure for responding to requests from data subjects is set out in figure 1 and expanded in table 1. The specifics of each step in the procedure will vary according to the type of request involved – refer to the relevant section of the procedure for more detail.

Step	Description	Person
Data Subject	The data subject submits a request via one of a number of methods, including electronically (via email or via our website), by letter, or on the telephone. This may be received by any part of the organisation but should ideally be channelled through customer services. A *Data Subject Request Form* is available for this purpose.	Data Co-Ordinator
Log data subject request	The fact that the request has been received is logged in the *Data Subject Request Register* and the date of the request recorded.	Data Co-Ordinator
Confirm identity of data subject	The identity of the data subject is confirmed via an approved method. More information may be requested to confirm identity if required. If the identity of the data subject cannot be confirmed, the request is rejected at the reason for this communicated to the data subject.	Data Co-Ordinator
Evaluate validity of request	The test of whether the request is *'manifestly unfounded or excessive'* is applied. If so, a decision is made whether to reject the request or apply a charge to it. In the case of requests for rectification, erasure, restriction of, or objection to, processing, a decision is also taken about whether the request is reasonable and lawful. If not, the request is rejected and the data subject informed of the decision and their right to complain to the supervisory authority.	Data Co-Ordinator Data Controller
Charge for request	If a charge is applied, the data subject is informed of the charge and has an opportunity to decide whether or not to proceed. If the data subject decides not to proceed, the request is rejected and the reasons communicated.	Data Co-Ordinator Data Controller
Compile Requested information	The relevant information is compiled according to the type of request. This may involve planning how the requested action, e.g. erasure or restriction of processing, will be achieved. A maximum of one month is permitted; if the request will take longer than that then a maximum of two further months are allowed and the data subject must be informed of the delay and the reasons for it within one month of the request being submitted.	Data Administrator Data Owner
Take requested action/provide requested information	The requested action is carried out (if applicable) and the information requested is provided to the data subject electronically, if that is the preferred method, or via other means.	Data Administrator
Close data subject request	The fact that the request has been responded to is logged in the *Data Subject Request Register*, together with the date of closure.	Data Administrator

APPLICABLE RIGHTS BASED ON LAWFUL BASIS OF PROCESSING

Right of the Data Subject	Basis of lawful processing					
	Consent	Contractual	Legal Obligation	Vital Interests	Public Interest	Legitimate Interest
Withdraw Consent	Yes	No	No	No	No	No
Be informed	Yes	Yes	Yes	Yes	Yes	Yes
Access	Yes	Yes	Yes	Yes	Yes	Yes
Rectification	Yes	Yes	Yes	Yes	Yes	Yes
Erasure	Yes	No	No	No	No	Yes
Restrict Processing	Yes	Yes	Yes	Yes	Yes	Yes
Data Portability	Yes	Yes	No	No	No	No
Object	N/A	No	No	No	Yes	Yes
Automated decision making and profiling	N/A	No	No	Yes	Yes	Yes



Data subject request procedure flowchart

The Right to Withdraw Consent
The Data Subject has the right to withdraw consent where the basis for processing of their personal data is that of consent (I.e. the processing is not based on a different justification allowed by the GDPR such as contractual or legal obligation).

Before excluding the data subject's personal data from processing, it may be confirmed that consent is indeed the basis of the processing. If not, then the request may be rejected on the grounds that the processing does not require the data subject's consent. Otherwise, the request should be allowed.

In many cases, the giving and withdrawal of consent will be available electronically I.e. Online, and this procedure will not be required.

Where consent involves a child, defined by their GDPR as aged 16+ (unless changed by law in individual member states) giving consent must be authorised by the holder of parental responsibility over the child.

The Right to Be Informed
At the point where, personal data are collected from the data subject or obtained from another source, there is a requirement to inform the data subject about our use of this data and their rights over it. Privacy notice procedure, which describes the information that must be provided and sets out how and when this might be achieved.

The Right of Access
A Data subject has the right to ask the organisation whether we process data about them, to have access to the data and in addition the following information: –

1. The purposes of the processing
2. The categories of the personal data concerns
3. The recipients, or categories of recipients of the data if any, in particular any third countries or international organisations
4. The length of time that personal data be stored for (or the criteria used to determine that period)
5. The data subject's rights to rectification or erasure of their personal data and restriction of, or objection to, its processing
6. The data subject's rights to lodge a complaint with a supervisory authority
7. Information about the source of the data, if not directly from the data subject
8. Whether the personal data will be subject to automated processing, including profiling and, if so, the logic and potential consequences involved.
9. Where the data are transferred to 1/3 country or international organisation, information about the safeguards that apply

In most cases the decision-making process for such requests will be straightforward unless it is judged that the request is manifestly unfounded or excessive. The compilation of the information is likely to require the input of the data owner.

The Right to Rectification
Where personal data is inaccurate the data subject has the right to request that it be corrected, and incomplete personal data completed based on information they may provide.

Where necessary, the organisation will take steps to validate the information provided – subject to ensure that it is accurate before amending it.

The Right to Erasure
Also known as the "right to be forgotten", the subject has the right to require the organisation to erase personal data about them without undue delay where one of the following applies: –

- The personal data are no longer necessary for the purpose for which they were collected
- The data subject withdraws consent and there is no other legal ground for processing
- The data subject objects to the processing of the personal data
- The personal data has been unlawfully processed
- For compliance reasons, I.e. To meet the legal obligations of the organisation
- Where the personal data was relevant to the data subject is a chance

Reasonable efforts must be made to ensure erasure where the personal data has been made public.

The organisation will need to make a decision on each case of such requests as to whether the request can or should be declined for one of the following reasons: –

- Right of freedom of expression and information
- Compliance with the legal obligation
- Public interest in the area of public health
- To protect archiving purposes in the public interest
- The personal data is relevant to a legal claim

It is likely that such decisions will require the involvement of the organisation's data protection personnel and in some cases senior management.

The Right to restrict processing
The data subject can exercise the right to restrict the processing of their personal data in one of the following circumstances: –

- Where the subject contests the accuracy of the data, until we have been able to verify its accuracy
- As an alternative to erasure in the circumstances where processing is unlawful
- Where the data subject needs the data for legal claims, but it is no longer required by us
- Whilst a decision on an objection to processing is pending

We will need to make a decision in each case of such requests as to whether the request should be allowed. It is likely that such decisions will require the involvement of the data protection contact person and, in some cases, senior management.

Where a restriction of processing is in place, the data may be stored but not processed without the data subjects consent, unless for legal reasons (in which case the data subject must be informed).

Other organisations who may process the data on our behalf must also be informed of the restriction.

The Right to Data Portability

The data subject has the right to request that their personal data have been provided to them in a "structured, commonly used and machine-readable format" (GDPR article 20) and to transfer that data to another party e.g. service provider. This applies to personal data for which processing is based on the data subject's consent and the processing carried out by automatic means.

Where feasible the database subjects can also request that the personal data be transferred directly from our systems to those of another provider.

For services that come under this category, little decision-making is required for each case and it is highly desirable that this process is automated in its execution.

The Right to Object

The data subject has the right to object to processing that is based on the following legal justifications: –

- For the performance of a task carried out in public interest are in the exercise of official authority vested in the controller
- For the purposes of the legitimate interests of the controller

Once an objection has been made, we must justify the grounds on which the processing is based and suspend processing until this is done. Where the personal data is used for direct marketing we have no choice but to no longer process the data.

Rights in relation to automated decision-making and profiling

The data subject is the right to not be the subject of automated decision-making the decision has a significant effect on them and can insist on human intervention where appropriate. The data subject also has the right to express their point of view and contest decisions.

There are exceptions to this right, which are if the decision: –

- Is necessary for a contract
- As authorised by law
- It is based on the data subjects explicit consent

In assessing these types of requests, a judgement needs to be made about whether the above exceptions apply in the particular case in question.

Summary of data subject rights by lawful basis of processing

The following table shows which rights of the data subject are relevant to each basis of lawful processing. It should be used as a general guide only, as the specific circumstances may affect the validity of the request.

Note

All of the above assume that: –

1. The personal data are being properly processed
2. The personal data are necessary in relation to the purposes for which they were collected or otherwise processed

If this is not the case, then further investigation must be made regarding the validity of the request.

8. Appendix 4 - The Lawfulness of Processing

There are six alternative ways in which the lawfulness of a specific case of processing of personal data may be established under the Regulation. It is our policy to identify the appropriate basis for processing and to document it in accordance with the regulation. The options are described in brief in the following sections: –

Consent
Unless it is necessary for a reason allowable in the GDPR, we will always obtain explicit consent from a data subject to collect and process their data. Transparent information about usage of their personal data will be provided to data subjects at the time that consent is obtained and their rights with regards to the data explained, such as the right to withdraw consent (where appropriate). If the personal data is not obtained directly from the data subject, then this information will be provided to the data subject within a reasonable period after the data is obtained and within one month.

Performance of a Contract
As referred to above where the personal data collected and processed is required to fulfil a contract such as a contract of employment with the data subject, explicit consent is not required. This will often be the case where the contract cannot be completed without the personal data in question.

Legal Obligation
If the personal data is required to be collected and processed in order to comply with the law, then explicit consent is not required. This will often be the case for some data related to employment and taxation for example. See Appendix 1 for data retention periods.

Vital interests of data subject
In a case where the personal data is required to protect the vital interests of the data subject or of another natural person, then this may be used as the lawful basis of the processing. In these circumstances we will retain reasonable documented evidence that this is the case, whenever this reason it is used as the lawful basis of processing of personal data.

Task Carried Out in the Public Interest
Where we need to perform a task that is in the public interest or as part of an official duty then the data subject's consent will not be requested. The assessment of the public interest or official duty will be documented and made available as evidence where required.

Legitimate Interests
If the processing of specific personal data is in the legitimate interests of the employment and this is judged not to affect the rights and freedoms of the data subject in a significant way, then this may be defined as the lawful reason for the processing. Again, the reasoning behind this view will be documented.

9. Appendix 5 - Job Application Privacy Notice

Your Consent

In order for the Organisation to accept your application form, you must provide consent for the Organisation to process your job application in line with the Privacy Notice regarding Job Applications.

This statement (the "Privacy Statement") aims to inform you of how the Organisation will use the information you submit when applying for a job at the Organisation ("Job Application Data"). All Job Application Data you submit to the Organisation is retained in the Organisation.

What types of information do we process?

This Privacy Statement covers any Job Application Data you submit to us, such as:

- Name, address, email address, telephone number, or other contact information;
- Information contained in your CV or cover letter, such as previous work experience, education, or other information you provide for our consideration;
- Type of employment sought, desired salary, willingness to relocate, or other job preferences, and
- Names and contact information for referrals

It is your responsibility to obtain consent from references before providing their personal information to us. For the avoidance of doubt, the Organisation does not wish to receive any confidential or proprietary (or patented) information which you have received from your previous employers.

Who may access your data?

Only select employees of the Organisation - such as your potential future manager(s), employees of the Human Resources Department, HR Duo HR and IT (for maintenance purposes only) - and select employees of our external service providers who support the Organisation with the administration of recruitment applications, have access to your Job Application Data.

The Organisation will not supply any data to any third party other than those identified above without your express authorization.

For what purposes will Job Application Data be used?

The Job Application Data you provide will be used to assess your application for employment at the Organisation, to verify your information and conduct reference checks, and to communicate with you.

If you accept employment with the Organisation the information collected will become part of your employment record and will be used for employment purposes.

How long will we keep your data?

Your Job Application Data is stored in our applicant's data base for 18 months as from your most recent submission of Job Application Data.