DATA PROTECTION HANDBOOK

RedRock Recruitment Limited

Version 1.2 - July 2018

Table of Contents

Data Protection Policy 4

About this Policy 4

Data Protection Principles 4

Lawfulness, Fairness & Transparency 5

Purpose Limitation 6

Data Minimisation 6

Accuracy 6

Storage Limitation 6

Security Integrity & Confidentiality 7

Transfer Limitation 7

Data Subject's Rights & Requests 7

Accountability 8

Direct Marketing 9

Sharing Personal Data 9

Information Security Policy 11

About This Policy 11

Information Security Training 11

Preventative Security Measures 11

Passwords & Network Access Rights 12

Shared Logins 12

Transmission of Data 13

Use of Portable Media 13

Use of Paper Records 13

Deletion of Personal Data from Company IT Equipment 14

Deletion of Personal Data from Personal Mobile Devices 14

Data Retention Policy 15

About This Policy 15

Location of Business Records 15

Keeping Information Up To Date 16

General Principles on Data Retention 16

Retention Period (External Data Subjects) 16

Retention Period (Internal Data Subjects) 17

Erasure Request Procedure 19
About this Procedure 19
External Data Subjects: 19
Internal Data Subjects: 20
Subject Access Request Procedure 22
About This Procedure 22
Receiving A SAR 22
Fees For Handling A SAR 22
Provision of Information 22
Extending the Time to Respond 23
Refusing A SAR 24
SAR – Standard Letter 1 - Acknowledgement 25
SAR – Standard Letter 2 – Detailed Response 26
Data Breach Procedure 28
About This Procedure 28
What Is A Data Breach? 28
Preventing Data Breaches 28
Steps To Take In The Event Of A Data Breach 29
Notifying the Information Commissioner's Office 29
Notifying The Individual 30
Data Breach – Standard Letter – Breach Notification to Individuals 32

Data Protection Policy

About this Policy

We hold personal data for several different Data Subjects within the ordinary course of our business activities. These include Candidates, Client Contacts, Referees, Supplier Contacts, Applicants and Employees.

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

This Data Protection Policy sets out the steps which we take to ensure the protection of all personal data and other confidential information which we use in the course of our business.

The Directors are responsible for overseeing this policy and ensuring its proper implementation within the business. However, all employees share the responsibility for ensuring that the information which we use in our business is kept securely.

Data Protection Principles

We adhere to the principles relating to processing of personal data set out in the GDPR which require personal data to be:

1. Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

2. Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

3. Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation).

4. Accurate and where necessary kept up to date (Accuracy).

5. Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is processed (Storage Limitation).

6. Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

7. Not transferred to another country without appropriate safeguards being in place (Transfer Limitation); and

8. Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

Lawfulness, Fairness & Transparency

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

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

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

1. The Data Subject has given his or her Consent;

2. The processing is necessary for the performance of a contract with the Data Subject;

3. To meet our legal compliance obligations;

4. To protect the Data Subject's vital interests;

5. To pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process personal data for legitimate interests are set out in our Privacy Notices.

The GDPR requires us to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through an appropriate Privacy Notice which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect personal data directly from Data Subjects, including for employment purposes, we must provide the Data Subject with all the information required by the GDPR including our identity, how and why we will use, process, disclose, protect and retain that Personal Data through a Privacy Notice which must be presented when the Data Subject first provides the personal data.

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

Purpose Limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

We cannot use personal data for new, different or incompatible purposes from that disclosed when it was first obtained unless we have informed the Data Subject of the new purposes and they have consented where necessary.

Data Minimisation

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

Staff members may only process personal data when performing their job duties requires it. Staff members cannot process personal data for any reason unrelated to their job duties.

When personal data is no longer needed for specified purposes, it must be deleted or anonymised in accordance with our Data Retention Policy.

Accuracy

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

All staff members must ensure that the personal data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. Staff members must check the accuracy of any personal data at the point of collection and at regular intervals afterwards. All reasonable steps must be taken to destroy or amend inaccurate or out-of-date personal data.

Storage Limitation

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

We must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

For further information, please refer to our Data Retention Policy.

Security Integrity & Confidentiality

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

We will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable).

We will regularly evaluate and test the effectiveness of the relevant safeguards to ensure security of our processing of Personal Data. For further information about the steps which we have taken, please refer to our Information Security Policy.

The GDPR requires data controllers to notify any Personal Data Breach to the ICO and, in certain instances, the Data Subject. We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects and/or the ICO where we are legally required to do so. For further information, please refer to our Data Breach Procedure.

Transfer Limitation

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. Personal data is transferred when it originates in one country and is transmitted to, send to, viewed in or accessed in a different country.

We shall only transfer Personal Data outside the EEA if one of the following conditions applies:

1. The European Commission has issued a decision confirming that the country to which we transfer the personal data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

2. Appropriate safeguards are in place such as binding corporate rules (BCR) or standard contractual clauses approved by the European Commission;

3. The Data Subject has provided explicit consent to the proposed transfer after being informed of any potential risks; or

4. The transfer is necessary for one of the other reasons set out in the GDPR.

Data Subject's Rights & Requests

We acknowledge that Data Subjects have rights when it comes to how we handle their personal data. These include rights to:

1. Withdraw consent to processing at any time;

2. Receive certain information about our processing activities;

3. Request access to the personal data that we hold;

4. Prevent our use of their Personal data for direct marketing purposes;

5. Ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

6. Restrict processing in specific circumstances;

7. Challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

8. Request a copy of an agreement under which personal data is transferred outside of the EEA;

9. Object to decisions based solely on Automated processing, including profiling (ADM);

10. Prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;

11. Be notified of a personal data Breach which is likely to result in high risk to their rights and freedoms;

12. Make a complaint to the ICO; and

13. In limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

Accountability

We acknowledge that we are obliged to implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. We are responsible for, and must be able to demonstrate, compliance with the data protection principles.

We must have adequate resources and controls in place to ensure and to document GDPR compliance including:

1. keeping and maintaining accurate records of our data processing activities and the legal bases upon which such processing is carried out;

2. implementing “Privacy by Design” when processing personal data and completing Data Privacy Impact Assessments where processing presents a high risk to rights and freedoms of Data Subjects;

3. integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices or Fair processing Notices;

4. regularly training our staff members on the GDPR and our policies on data protection. We shall maintain a record of training which is attended or completed by our staff members; and

5. regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

Direct Marketing

In general terms, most of the communications which we are likely to send to our Data Subjects fall within the scope of the actual services which we are providing and are not marketing communications. However, in some cases we may wish to send marketing communications.

We acknowledge that we are subject to certain rules and privacy laws when marketing to our customers.

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

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

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

Sharing Personal Data

Generally, we are not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

We shall only share the personal data we hold with another employee, agent or representative of our group if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

We shall only share the personal data we hold with our service providers if:

1. They have a need to know the information for the purposes of providing the contracted services;

2. Sharing the personal data complies with the Privacy Notice provided to the Data Subject;

3. The third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

4. The transfer complies with any applicable cross border transfer restrictions; and

5. A fully executed written contract with appropriate third party clauses has been obtained.

Due to the nature of our business, we will frequently share information with third parties for legitimate business reasons. Our Privacy Notices specify the parties with whom we shall share personal data. We shall seek express sharing consent whenever we need to share:

1. A Candidate's personal data with a Client;

2. A Client Contact's personal data with a Candidate; or

3. A Referee's personal data with a Client.

Information Security Policy

About This Policy

This Information Security Policy sets out the steps which we take to ensure the protection of all personal data and other confidential information which we use in the course of our business.

The Directors are responsible for overseeing this policy and ensuring its proper implementation within the business. However, all employees share the responsibility for ensuring that the information which we use in our business is kept securely.

Information Security Training

We take active steps to ensure that all staff members are aware of the expectations upon them in respect of Information Security.

We will ensure that appropriate training is carried out on commencement of employment and then not less than once every 12 months. Where it is particularly appropriate to the individual's job role, we will arrange for additional Information Security training to be carried out as and when necessary.

Preventative Security Measures

We have implemented appropriate technical measures to ensure the security and integrity of our IT services environment. This includes:

- [Installation of a [hardware] firewall at the network router level]
- [Installation and regular updates of TYPE anti-virus and anti-malware software on all local machines]
- [Regular, forced updates of all desktops and laptops with the latest OS version releases]
- [Encryption of all [desktops and] laptops to prevent unauthorised access in the event of loss or theft]
- [Mandating suitably complex network access passwords]
- [Implementation of two-factor authentication for login to Office 365]
- [Regularly scheduled penetration testing of our network by our IT services providers to minimise the risk of third-party intrusion.]
- [Secure destruction of IT services equipment upon disposal.]
- [Encryption of all local storage media]

- [Prevention/limitation of ability to extract personal data from our CRM without authorisation.]
- [Prevention of access to file-sharing and internet email websites without authorisation.]
- [Implementation of SSL certificate on our website, URL, to protect data which is transmitted by third parties.]
- [Protection of company website through the use of Content Delivery, DDoS mitigation and internet security tools.]

Passwords & Network Access Rights

We ensure that individuals within our business are given access rights which are appropriate to the level at which they work. In general terms, directors and support staff shall be given full administration rights whereas other staff members will be given standard access rights.

For access rights to be effective, it is important that network and system passwords are not shared between staff members. For example, staff members should not give any colleague access to their network login for email monitoring purposes but, where appropriate, should arrange delegate access through the email client settings.

All staff members must change their network passwords not less than once every XX days. Network passwords should be suitably complex with a combination of uppercase and lowercase letters, numbers and special characters.

On termination of any staff member's employment, all network and system access passwords must be immediately deleted or changed to prevent unauthorised access. This includes access to company systems and third-party websites/databases.

Shared Logins

In limited circumstances, it is necessary for staff members to share access to an external information technology resource e.g. a database or job board.

It would be a breach of contract and potentially a criminal offence for any former employee to access any external information technology resource using company login credentials. However, we will also take active steps to minimise the risk of this happening.

If access credentials to an external resource are shared for any reason, these credentials must be changed (i) immediately upon the termination of any relevant staff member's employment and (ii) in any event, at least once every XX months.

Transmission of Data

We acknowledge that email is not considered to be a secure method of sending large quantities of personal data.

We therefore acknowledge the need to consider whether email is the most appropriate way of sending large volumes of personal data or personal data which is particularly sensitive in nature and:

1. If email is not appropriate under the circumstances, we will endeavour to use another form of secure data transfer from time to time e.g. one which utilises secure FTP; or

2. If email is the only practical way of sending personal data, we will take steps to secure the personal data from accidental loss or deliberate interception by password-protecting and/or encrypting the relevant files and providing such password or encryption key to the proper recipient in a separate communication.

Use of Portable Media

We generally discourage the use of portable media for the storage or transfer of personal data. Once personal data is transferred onto a USB stick, DVD-R or similar format, the risk of accidental loss or theft of such personal data is significantly higher.

Where any staff member needs to transfer personal data onto any portable media:

1. This must be for legitimate, justifiable business reasons;

2. A Director must have given prior written approval to such transfer; and

3. The portable media must be protected by 256-bit encryption or, if that is not possible, it must at minimum be password-protected with a suitably complex password incorporating a combination of uppercase and lowercase letters, numbers and special characters.

Use of Paper Records

We aim to be as paper-free as reasonably possible. This is not only important for personal data security but is also in keeping with our Environmental Policy. We do however acknowledge that paper copies of documents and personal data will inevitably be used within our offices. With this in mind:

1. Staff members should observe a clear desk policy and not keep paper records on their desk other than those which are relevant to their current tasks.

2. Any particularly sensitive paper records, such as DBS disclosures, must be kept in a locked filing cabinet or drawer and securely destroyed once they are no longer required.

3. Paper records should only be removed from our offices for legitimate business reasons e.g. a Candidate's CV could be taken to a Client meeting.

4. Paper records should not be retained for longer than they are reasonably required. All staff members should regularly review the paper records which they have in their possession and [shred them securely] or [place them in the confidential waste bins for secure destruction.]

Deletion of Personal Data from Company IT Equipment

If any item of IT equipment (including desktops, laptops, mobile telephones and tablets) is no longer required:

1. Where the device is to be sold or donated to a third-party organisation, we shall ensure the security of any personal data saved or cached on such device by securely wiping such device using:

    a. The appropriate device reset option in the case of a mobile telephone or tablet;

    b. Commercial-grade data deletion software in the case of a desktop or tablet;

2. Where the device is inoperative or obsolete, ensuring that the storage media on such device is physically destroyed so that the data may not be recovered. Wherever possible, we shall use a third party secure data deletion service for this and require a certificate of destruction from such third party.

Deletion of Personal Data from Personal Mobile Devices

Due to the nature of the industry in which we operate, it is common for staff members to contact Client Contacts, Candidates and other data subjects using their own mobile device. Whilst this is not something which we prevent - unless we have provided a company mobile device for the relevant member of staff to use - we acknowledge that this may lead to our employees holding confidential information and personal data on their own devices.

We require all employees to confirm (i) that their personal devices are secured by a PIN or fingerprint control and (ii) that they will, on demand, delete all personal data from their personal mobile devices and show that they have done so. All employees are aware that any unauthorised retention of personal data on their mobile device:

- May be gross misconduct and/or a serious breach of contract
- Will, in some cases, be an offence under s170 of the Data Protection Act 2018
- May entitle the company to seek injunctive relief

Data Retention Policy

About This Policy

This Data Retention Policy relates to the business records which we control in relation to (i) external Data Subjects, such as Candidates, Client Contacts, Referees and Supplier Contacts and (ii) internal Data Subjects, such as Applicants and Employees.

The policy is intended to ensure that we process our business records in accordance with the personal data protection principles, in particular that:

- Personal data must be collected only for specified and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.

- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When personal data is no longer needed for specified purposes, it is deleted or anonymised as provided by this policy.

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

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

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

The Directors are responsible for overseeing this policy. Any questions about the operation of this policy should be submitted to a Director.

Location of Business Records

Our business records are mainly stored within our CRM/database, NAME.

We store our internal HR records in NAME.

We may also store business records:

- On our internal network in shared folders;

- On mobile devices belonging to the Company;

- In cloud-based storage services such as OneDrive and Dropbox.

Keeping Information Up To Date

We acknowledge the need to ensure that our records are kept up to date and accurate.

Our Employees are trained to update Data Subjects' records whenever appropriate to ensure that (i) the data is up to date and (ii) all relevant employees are able to access and use such data for legitimate business purposes.

Employees are actively encouraged to keep the company up to date with any changes to their own name, address, personal contact information and Next of Kin details. These details are reviewed and confirmed not less than once every year.

General Principles on Data Retention

We acknowledge the need to manage and retain business records in accordance with the data protection principles referred to in this policy and, in particular, to ensure that:

- Business records are regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary to be used for the purpose for which they were recorded.

- Business records are kept secure and are protected against unauthorised or unlawful processing and against accidental loss, destruction or damage.

- When records are destroyed, whether held as paper records or in electronic format, we will ensure that they are safely and permanently erased.

Retention Period (External Data Subjects)

1. Our standard data retention period is three years from the last date on which we were in actual contact with the relevant Data Subject.

2. If more than three years have elapsed since we were last in contact with the Data Subject (**Expiry Date**), our process is to delete the personal data relating to such Data Subject, subject to paragraph 3 below.

3. If the Data Subject is a Candidate who we have placed with a Client, we will usually retain the Candidate's personal data for a period of seven years from the date on which the Candidate was placed with the Client (Legal Retention Period). The reasons for the Legal Retention Period are:

    a. That the usual contract limitation period is six years and we could be required to defend ourselves against a breach of contract claim at any time during the limitation period.

    b. It is a common provision in Client agreements that we must for a period of not less than six years retain complete records of the activities which were carried out in the course of performing the contract; and

c. If we have placed the Candidate in a temporary role, we are required by HMRC to retain a full audit trail of payments and receipts in respect of such temporary supply for the remainder of the relevant financial year plus a further six years i.e. up to seven years in total.

4. Where the Expiry Date has passed but we are required to keep relevant data for the Legal Retention Period:

   a. Any personal data which is not needed for audit or legal defence purposes must be removed from the Data Subject's record. This includes personal data which is (i) irrelevant (ii) out of date and/or (iii) particularly confidential in nature, such as a DBS Disclosure document.

   b. The Data Subject's data shall not be used in the course of usual recruitment activities but shall instead be marked as Archived/Pending Deletion for the remainder of the Legal Retention Period.

   c. Contact with the Data Subject might be re-established in the ordinary course of business, although this must not be through the active use of data which is marked as Archived/Pending Deletion. Where contact is re-established, [the Data Subject's original record may be marked as Active once again but any irrelevant and/or expired data must be removed from the business record to ensure that it remains up to date and relevant] or [we shall create a new record for the Data Subject].

5. In some instances, a Data Subject's record will not reach the Expiry Date because we stay in regular contact with such Data Subject. Although the record itself shall not expire under these circumstances, we shall take active steps to ensure that the personal data within the Business Record remains relevant and necessary for the purpose for which it was obtained. We shall delete any documents, notes and other types of personal data which are no longer relevant or necessary.

Retention Period (Internal Data Subjects)

Recruitment:

1. We retain recruitment-related information to demonstrate, if necessary, that Applicants have not been discriminated against on prohibited grounds and that our internal recruitment is conducted in a fair and transparent way.

2. Our internal Privacy Notice sets out how long we expect to keep their personal information once a recruitment decision has been communicated to them. This is usually for twelve months from the communication of the outcome of the recruitment exercise, which takes account of both the time limit to bring claims and for claims to be received by us.

3. Information relating to successful Applicants will be transferred to their employment record. This will be limited to that information necessary for the working relationship and, where applicable, that required by law.

Employment:

1. Our standard Data Retention Period in respect of Employees is seven years from termination of the employment relationship. The reason for this is that:

    a. the usual contract limitation period is six years and we could be required to defend ourselves against a breach of contract claim at any time during the limitation period; and

    b. we are required by HMRC to retain fully auditable payroll records for the remainder of the relevant financial year plus a further six years i.e. up to seven years in total.

2. Where appropriate, we shall delete any information which is no longer required for audit/legal compliance purposes on termination of an Employee's employment.

Erasure Request Procedure

About this Procedure

We acknowledge that a Data Subject is entitled to submit a request for erasure of their details from time to time (**Erasure Request**) i.e. the right to be forgotten.

The right to make an Erasure Request applies to both (i) external Data Subjects, such as Candidates, Client Contacts, Referees and Supplier Contacts and (ii) internal Data Subjects, such as Applicants and Employees. However, the extent to which we can comply with an Erasure Request shall vary, depending on the type of Data Subject.

External Data Subjects:

Upon receipt of an Erasure Request, we shall:

1. Verify the identity of the Data Subject; and

2. If appropriate, check whether the Data Subject wishes (1) to be erased from our business records or (2) to remain within our business records but marked as Non-Active or Do Not Contact.

If the Data Subject wishes to have their personal data **Erased**:

1. We shall consider whether there is any lawful reason or legal requirement to retain the personal data as:

    a. The Conduct of Employment Agencies and Employment Businesses Regulations 2003 require us to keep records of any work-finding services which we have provided for not less than 12 months.

    b. If we have placed the Data Subject in a permanent role or on a temporary assignment, we will usually retain any relevant personal data for seven years so that we can defend ourselves from any legal claim which may arise and maintain auditable records for tax compliance reasons.

2. We shall within one month of receiving the Erasure Request, confirm the outcome of such Erasure Request, the steps which we have taken and the extent to which any personal data has been retained.

3. If we have retained personal data for any reason, this shall not be used for recruitment purposes and the relevant Data Record shall be [removed from our front-office database system] or [marked as Pending Deletion].

4. We shall ensure that any (i) joint Data Controller or (ii) third party which is processing relevant Data Subject's data on our behalf is informed that the Data Subject has made an Erasure Request and takes appropriate steps to comply with such Erasure Request.

5. If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

6. If we are not going to respond to the request, we shall inform the Data Subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

If the Data Subject does not wish to have their personal data erased but would prefer to have their record marked as **Do Not Contact**, we shall record this in the relevant data record.

Once marked as Do Not Contact:

1. The Data Subject's record shall then be subject to our standard data retention procedures; and

2. Will be deleted after three years or more of inactivity, subject to any legal right or obligation for us to retain the data for compliance purposes.

Internal Data Subjects:

An Internal Data Subject has a limited right to make an Erasure Request where:

a) The personal data is no longer necessary for the purpose which we originally collected or processed it;

b) We have processed the personal data unlawfully; or

c) There is a legal obligation for the personal data to be erased e.g. a court order.

If we receive an Erasure Request from any Internal Data Subject:

1. We shall verify the Data Subject's identity where appropriate. This will not usually be necessary for current employees.

2. We shall acknowledge the request in writing and then, within one month of receiving the Erasure Request, confirm the outcome of such Erasure Request.

3. If appropriate, we shall ensure that any (i) joint Data Controller or (ii) third party which is processing relevant Data Subject's data on our behalf is informed that the Data Subject has made an Erasure Request and takes appropriate steps to comply with such Erasure Request.

4. If the request is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of erasure, or refuse to act on the request.

5. If we are not going to respond to the request, we shall inform the Data Subject of the reasons for not taking action and of the possibility of lodging a complaint with the ICO.

Subject Access Request Procedure

About This Procedure

This Subject Access Request Procedure sets out our procedure in relation to any Subject Access Request which we may receive from a Data Subject.

The Directors are responsible for overseeing this procedure. Any questions about the operation of this procedure should be submitted to a Director.

Receiving A SAR

Data Subjects have the right to request access to their personal data processed by us. Such requests are called subject access requests (**SARs**).

When a Data Subject makes a SAR, we shall take the following steps:

1. Acknowledge the SAR in writing, by using Standard Letter 1

2. Log the date on which the request was received (to ensure that the relevant timeframe of one month for responding to the request is met);

3. Confirm the identity of the Data Subject who is the subject of the personal data. For example, we may request additional information from the Data Subject to confirm their identity;

4. Search databases, systems, applications and other places where the personal data which are the subject of the request may be held; and

5. Confirm to the Data Subject whether or not personal data of the Data Subject making the SAR are being processed. The outcome of the SAR shall usually be confirmed in Standard Letter 2.

Fees For Handling A SAR

We shall not usually charge a fee to the Data Subject for carrying out a SAR (i.e. as the previous statutory £10 fee is no longer in force.)

If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may charge a reasonable fee, taking into account the administrative costs of providing the personal data.

Provision of Information

If personal data of the Data Subject are being processed, we shall provide the Data Subject with the following information in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in writing or by other (including electronic) means:

- the purposes of the processing;

- the categories of personal data concerned (for example, contact details, bank account information and details of sales activity);

- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients overseas (for example, US-based service providers);

- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

- the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data or to object to such processing;

- the right to lodge a complaint with the Information Commissioner's Office (ICO);

- where the personal data are not collected from the Data Subject, any available information as to their source;

- the existence of automated decision-making and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Data Subject; and

- where personal data are transferred outside the EU, details of the appropriate safeguards to protect the personal data.

We shall also, unless there is an exemption, provide the Data Subject with a copy of the personal data processed by us in a commonly used electronic form e.g. PDF documents, unless the Data Subject either did not make the request by electronic means or has specifically requested not to be provided with the copy in electronic form. We shall usually submit the data to the Data Subject within **one month** of receipt of the request.

Before providing the personal data to the Data Subject making the SAR, we shall review the personal data requested to see if they contain the personal data of other Data Subjects. If they do, we may redact the personal data of those other Data Subjects prior to providing the Data Subject with their personal data, unless those other Data Subjects have consented to the disclosure of their personal data.

Extending the Time to Respond

If the request is complex, or there are a number of requests, we may extend the period for responding by a further two months. If we extend the period for responding, we shall inform the Data Subject within one month of receipt of the request and explain the reason(s) for the delay.

Refusing A SAR

If the SAR is manifestly unfounded or excessive, for example, because of its repetitive character, we may refuse to act on the request. It would be unusual for us to refuse to act upon a SAR but may be appropriate if we consider the SAR to have been made in a vexatious or malicious manner to cause disruption to our business.

If we are not going to respond to the SAR, we shall inform the Data Subject of the reason(s) for not taking action and of the right to lodge a complaint with the ICO.

SAR – Standard Letter 1 - Acknowledgement

[On headed notepaper]

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

[DATE]

Dear [SALUTATION],

ACKNOWLEDGMENT OF YOUR DATA SUBJECT REQUEST

I write to acknowledge receipt of your data subject access request which we received on [DATE].

[We intend to respond to your request as soon as possible but will respond at the latest within one month from date of receipt. OR We have given some initial consideration to your request and realise that it will involve looking extensively at a high volume of emails and other documents. [We have not searched fully but anticipate that there may be some [NUMBER] emails and [NUMBER] documents to review.] Where our search brings up personal data not only about you but also others, we will have to consider whether to supply the data, and if so, whether on a redacted basis.

Because we consider that dealing with your request will be time-consuming, we will need to extend the time for responding. At the latest we will respond within three months of the request but will do our best to respond earlier.]

[NAME] will be responsible for overseeing the response to your request. If you have any questions about your request, please contact them.

[I also acknowledge receipt of the copy of your [driving licence OR passport] as confirmation of your identity. OR I would be grateful if you could provide confirmation of your identity. This should be in the form of a certified copy of your driving licence or passport.]

[To help us to deal with the request, it would help us if you could provide us with further information so that we could narrow the scope of our search. In particular, please could you state more specifically [whether your request relates to particular issues or incidents and/or dates. It would also be helpful if, in relation to emails, you could indicate the names of senders, recipients and approximate dates (if you know them].

Yours sincerely

SAR – Standard Letter 2 – Detailed Response

[On headed notepaper]

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

[DATE]

Dear [SALUTATION],

RESPONSE TO YOUR DATA SUBJECT ACCESS REQUEST DATED [DATE OF REQUEST]

We write further to your subject access request and our acknowledgment letter of [DATE].

We now [attach]/[enclose] copies of the personal data which we hold relating to you.

Your rights in connection with personal data

You may be interested to know of certain rights that you have in connection with your personal data. In particular, you have the right to correct the personal data that we hold about you or restrict the processing of your personal data under certain circumstances. You may also, under certain circumstances, have the right to object to the processing or to request erasure of your personal data.

You also have the right to make a complaint to the data protection supervisory authority in the UK, the Information Commissioner. For further information, see the Information Commissioner's Office website at *https://ico.org.uk/concerns/*.

We can confirm the following in respect of the data existing on the date your request was made:

1. THE PURPOSES FOR WHICH THE PERSONAL DATA IS PROCESSED
   [LIST OF PURPOSES]

2. THE CATEGORIES OF PERSONAL DATA CONCERNED
   [LIST OF CATEGORIES OF PERSONAL DATA]

3. THE RECIPIENTS OR CATEGORIES OF RECIPIENTS TO WHOM THE PERSONAL DATA HAVE OR MAY HAVE BEEN DISCLOSED
   [LIST OF RECIPIENTS (BY NAME OR GENERIC CLASS) TO WHOM DATA DISCLOSED]
   [LIST OF RECIPIENTS IN COUNTRIES OUTSIDE THE EEA OR INTERNATIONAL ORGANISATIONS]

4. SAFEGUARDS IN PLACE IN RELATION TO PERSONAL DATA TRANSFERRED TO THIRD COUNTRIES OR TO AN INTERNATIONAL ORGANISATION

[STATE WHETHER THERE IS AN ADEQUACY DECISION FROM THE EU COMMISSION IN RESPECT OF THIRD COUNTRY OR INTERNATIONAL ORGANISATION]
[LIST OF SAFEGUARDS IF NO ADEQUACY DECISION]

5. THE PERIOD FOR WHICH PERSONAL DATA WILL BE STORED OR CRITERIA USED TO DETERMINE THAT PERIOD
   [LIST OF CATEGORIES OF DATA AND PERIOD STORED OR CRITERIA USED TO DETERMINE THAT PERIOD]

6. SOURCE(S) OF THE DATA, WHERE APPLICABLE
   [IDENTIFY SOURCES OF DATA HELD]

   Some names and identifying particulars have been deleted to protect the identity of third parties.

7. THE EXISTENCE OF ANY AUTOMATED DECISION-MAKING
   [IDENTIFY ANY AUTOMATED DECISION-MAKING, INCLUDING PROFILING, AND ANY MEANINGFUL INFORMATION ABOUT THE LOGIC INVOLVED, ANY SIGNIFICANCE OR ENVISAGED CONSEQUENCES]

Some personal data has been omitted for the following reasons:

- [It is subject to legal privilege.]
- [It consists of a confidential reference given by us for employment purposes.]
- [It consists of records of intentions in relation to negotiations between us and you, disclosure of which we consider would be likely to prejudice those negotiations.]
- [It consists of health records and we consider that disclosure would be likely to cause serious harm to another person.]]

We have done our best to respond to your request and hope that you have found our approach helpful. You will see that when providing copies of personal data, we have sometimes gone beyond what is required in that not all of the information provided, strictly speaking, constitutes personal data relating to you.

Please do not hesitate to contact us if you have any questions about the contents of this letter.

Yours sincerely

Data Breach Procedure

About This Procedure

This policy sets out the procedure which we will follow in the event of a Data Breach.

The Directors are responsible for overseeing this procedure. Any questions about the operation of this procedure should be submitted to a Director.

What Is A Data Breach?

A Data Breach may take various forms but often involves the unauthorised disclosure of personal data to a third party. Data Breaches might typically occur when someone:

- Accidentally sends personal data to the incorrect party;
- Accidentally leaves confidential documents on a train;
- Has a laptop containing personal data stolen from their bag or vehicle;
- Deliberately extracts information from our database and transfers it out of our business;
- Hacks into our computer network to remove confidential or sensitive information; or
- Throws away company records without ensuring that they are shredded or otherwise destroyed.

A Data Breach could also involve the accidental or unlawful destruction, alteration or loss of access to Personal Data. This means that, for example, deliberate tampering with a Data Record by an employee would be a Data Breach, even if the Personal Data is not transferred anywhere.

Preventing Data Breaches

We take active steps to avoid Data Breaches by:

- Training our staff members about the importance of Data Security and the potential financial and reputational damage which can result from a Data Breach; and
- Putting in place technical and organisational measures to minimise the risk of a Data Breach occurring.

We do however acknowledge that, even if we take active steps to prevent breaches, they may still occur through human error or malicious conduct.

Steps To Take In The Event Of A Data Breach

1. If you become aware of a Data Breach, you **must** take action. You must not ignore the issue or try to hide it. You must therefore notify a Director without delay.

2. You must preserve all evidence of the Data Breach and do nothing that might compromise any enquiry or investigation in relation to such Data Breach.

3. The Director must arrange for a full investigation into the Data Breach without delay. Whilst the overall responsibility rests with the Director to ensure that this investigation is carried out, any relevant members of staff may be required to co-operate with the investigatory process.

4. The investigation must be carried out as quickly as possible. There is a 72 hour deadline to report the breach to the Information Commissioner's Office, where applicable.

5. On completion of the initial investigation into the Data Breach, the Director shall keep a record of the investigation and outcome in the company's central Data Protection file. This information shall be used to determine whether we need to disclose the Data Breach to:

    a. The Information Commissioner's Office, which is the supervisory authority in the UK; and/or

    b. The individual Data Subjects whose Personal Data was the subject of the Data Breach.

Notifying the Information Commissioner's Office

Recital 85 of the GDPR gives the following guidance on the risk to rights and freedoms:

A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.

The Director must determine whether the Data Breach is likely to result in a risk to the rights and freedoms of the Data Subjects affected by the breach.

In reaching a decision, the Director shall assess the following factors:

- Type of breach.
- Nature, sensitivity and volume of personal data.
- Ease of identification of individuals.
- Severity of consequences for individuals.

- Special characteristics of the individual (for example, vulnerable individuals may be at greater risk).
- Number of individuals affected.

The decision as to whether or not to report the breach **must be recorded in the company's Central Data Protection file.**

If the Director concludes that the Data Breach should be reported to the Information Commissioner's Office, the ICO's reporting process at: https://ico.org.uk/for-organisations/report-a-breach/ must be followed. This must happen within **72 hours** of the Data Breach occurring.

The ICO will typically require the following information:

- A description of the nature of the personal data breach including, where possible:
- The categories and approximate number of individuals concerned; and
- The categories and approximate number of personal data records concerned;
- The name and contact details of the data protection officer or other contact point where more information can be obtained;
- A description of the likely consequences of the personal data breach; and
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.

Notifying The Individual

The requirement to communicate a breach to individuals is triggered where a breach is likely to result in a high risk to their rights and freedoms. The threshold for communicating a breach to individuals is therefore higher than for notifying the ICO. In practice, where notification to individuals is required, notification to the ICO will always be required.

Although the deadline for notifying the ICO is set at 72 hours by law, there is no fixed deadline for notifying individuals. Notification must occur without undue delay.

Whether individuals should be notified will depend on the circumstances of the breach. For example, a loss of data which can be confirmed as encrypted and where the encryption key has not been compromised, may represent a very low risk, and would not require notification to individuals (or the ICO). However, even where data is encrypted, if there are no comprehensive backups of the data, then this could have negative consequences for individuals and notification may be appropriate.

The following information should be included in a breach notification to individuals:

- The name and contact details of the data protection officer (if applicable) or other contact point where more information can be obtained.

- A description of the likely consequences of the personal data breach.

- A description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, actions taken to mitigate any possible adverse effects.

After notifying individuals of a Data Breach, it is inevitable that some individuals will have further questions or significant concerns about the security of their data. Whilst there is nothing to stop any individual taking further action after a Data Breach, it is less likely that they will do so if their concerns are dealt with appropriately. With this in mind, any enquiries from affected individuals must be:

- Logged in the company's Central Data Protection record;

- Promptly acknowledged in writing; and

- Responded to, in full and courteously, without undue delay.

Data Breach – Standard Letter – Breach Notification to Individuals

[ON HEADED NOTEPAPER]

[ADDRESSEE]
[ADDRESS LINE 1]
[ADDRESS LINE 2]
[POSTCODE]

[DATE]

Dear [SALUTATION],

NOTIFICATION OF A PERSONAL DATA BREACH

We are sorry to inform you of a breach of security that has resulted in the [loss of OR unauthorised disclosure of OR unauthorised access to OR alteration of OR destruction of OR corruption of] your personal data.

The breach was discovered on [DATE] and is likely to have taken place on [DATE].

As a result of our investigation of the breach, we have concluded that:

The breach affects the following types of information:

TYPES OF INFORMATION, FOR EXAMPLE, FINANCIAL, SPECIAL CATEGORY DATA, CRIMINAL OFFENCE DATA].

The information has been [accidentally or unlawfully destroyed OR corrupted OR lost OR altered OR disclosed without authorisation OR accessed by [[NAME OR DESCRIPTION OF ORGANISATION] OR an unauthorised person]].

The breach occurred under the following circumstances and for the following reasons:

[CIRCUMSTANCES], [REASONS].

We have taken the following steps to mitigate any adverse effects of the breach:

[STEPS TAKEN].

We recommend that you take the following measures to mitigate possible adverse effects of the breach:

[MEASURES].

[We informed the Information Commissioner's Office of the breach on [DATE].]

You can obtain more information about the data breach from NAME, TITLE, EMAIL, TELEPHONE.

We apologise for any inconvenience that this breach may cause you. If you would like to discuss this matter with us, please let us know.

Yours sincerely