
BEYOND
ENCRYPTION

# OUR MISSION STATEMENT

To Secure Your…

- Communication…
- Data…
- Identity

# Data Protection Policy
# ISO 007

## Version 2

# Document Control

## Document Information

| | |
|---|---|
| **Document Author** | **Paul Holland** |
| **Next** | **Huw Thomas** |
| **Retention Period** | |

## Version History

| **Tool Used** | **Microsoft Word** | | |
|---|---|---|---|
| **Version** | **Date** | **Changed by** | **Comments** |
| **2** | **10.10.18** | **Huw Thomas** | **ISO Update** |
| | | | |
| | | | |

## Issue Control

| | |
|---|---|
| **Owner and Approver** | **Huw Thomas** |
| **Role** | **Quality and Compliance Manager** |
| **Signature** | |
| **Date** | **10.10.18** |

# Data Protection Policy

## Contents

# Data Protection Policy

## 1. Definitions

In this Policy, where a phrase uses 'Capital Letters', it is a defined term and has the meaning set out below. We recommend you refer to this section as you read through the Policy.

***Anonymised or Anonymising*****:** amending data so that the identity of the individual it concerns is permanently removed.

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

***Automated Processing***: any form of automated processing of Personal Data where an individual's Personal Data is used to evaluate them. This includes where the processing is used to analyse or predict the individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

***Company***: Beyond Encryption Limited (company number 08814096) of 1 Gloster Court, Whittle Avenue, Fareham, Hampshire, England, PO15 5SH.

***Company Personnel***: all employees, workers, contractors, agency workers, consultants, directors and members.

***Consent***: agreement which must be freely given, specific, informed and unambiguous. Consent is an indication of the Data Subject's wishes that they, by a statement or by a clear positive action, agree to the Processing of Personal Data relating to them.

***Data Controller***: the person or organisation that determines when, why and how to process Personal Data. The Data Controller is responsible for establishing practices and policies which conform to the GDPR and data protection law. We are the Data Controller of all Personal Data relating to Company Personnel and Personal Data used in our business for our own commercial purposes.

***Data Subject***: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country (i.e. they do not need to be within the EU and/or UK).

***Data Privacy Impact Assessment (DPIA)***: a specific type of assessment used to identify and reduce the risks associated with a data processing activity. A DPIA is often carried out as part of Privacy by Design.

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

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

***General Data Protection Regulation (GDPR)***: The General Data Protection Regulation (*(EU) 2016/679*). The GDPR applies to England and Wales from 25 May 2018 onwards. For the avoidance of doubt, Brexit will not affect the implementation date of the GDPR.

***Information Commissioner's Office (ICO)***: the data protection regulator in the UK, whose website is http://ico.org.uk. The ICO has useful guidance on its website which compliments this Policy.

***Personal Data***: means:

(i) any information identifying a Data Subject; or

(ii) any information relating to a Data Subject and we can identify that Data Subject (directly or indirectly) from:

a. that information alone; or

b. by combining that information with other identifying information, we possess or can reasonably access.

Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes Anonymous data. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

***Personal Data Breach***: any act or omission that compromises:

(i) the security, confidentiality, integrity or availability of Personal Data; or

(ii) the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect that data.

The loss or unauthorised access, disclosure or acquisition of Personal Data is a Personal Data Breach

***Policy***: This Data Protection Policy.

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

***Privacy Notices***: separate notices setting out information that may be provided to Data Subjects when the Company collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or a website privacy policy) or they may be stand-alone, one-time privacy statements

covering Processing related to a specific purpose. Privacy Notices are also sometimes called 'Privacy Policies'.

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

***Pseudonymisation or Pseudonymised***: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the Data Subject cannot be identified without the use of additional information (like a written 'key') which is meant to be kept separately and secure. Pseudonymised data is usually Personal Data because the Company has access (or can reasonably access) both the pseudonymised information and the 'key'

***Responsible Person***: an organisation can appoint a data protection officer to lead data protection compliance within its business. We are not legally required to appoint a data protection officer but have instead nominated the Responsible Person for Quality and Compliance to act as a central point of contact for matters of data protection within the Company. The person within the Company who acts as a central point of contact for all matters relating to data protection. Their details are: Huw Thomas, Quality and Compliance Administrator, Huw.Thomas@Beyondencryption.com.

***Sensitive Personal Data***: information revealing an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. Sensitive Personal Data also includes Personal Data relating to criminal offences and convictions.

# Data Protection Policy

## 2. Introduction

This Policy sets out how Beyond Encryption Limited ("**we**", "**our**", "**us**", the "**Company**") handles the Personal Data of Company Personnel, our customers, our suppliers and other third parties.

This Policy applies to:

all Personal Data we Process; and

all Company Personnel ("**you**", "**your**").

You must read, understand and comply with this Policy when Processing Personal Data on our behalf and attend training on its requirements.

Personal Data can be stored on any medium (e.g. on paper or electronically). Personal Data can also refer to past or present Data Subjects. This includes current or former Company Personnel, customers, client or supplier contacts, shareholders and website users of the Company.

This Policy sets out what we expect from you for the Company to comply with the GDPR and data protection law. **Your compliance with this Policy is mandatory.** Any breach of this Policy may result in disciplinary action.

This Policy is a confidential internal document. It must not be shared with third parties, clients or regulators without prior authorisation from the Responsible Person.

## 3. Scope

Compliance with data protection law is a key part of our business plan. By treating Personal Data correctly and lawfully, we are protecting the confidence that our staff, customers and third parties have in our business, as well as protecting our reputation in the marketplace.

Safeguarding the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Company is 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 e to comply with the provisions of the GDPR.

All managers are responsible for ensuring that all Company Personnel comply with this Policy. Managers must implement appropriate practices, processes, controls and training to ensure universal compliance within the business.

The Quality and Compliance Manager is responsible for overseeing this Policy. The Responsible Person's role is to coordinate the Company's data protection compliance within the Company but, for the avoidance of doubt, everybody has responsibility for following this Policy in their day-to-day activities.

## 4. Contacting the Responsible Person

Please contact the Quality and Compliance Manager with any questions about the operation of this Policy or if you have any concerns that this Policy is not currently being followed.

You must always contact the Quality and Compliance Manager in the following circumstances:

- if you are unsure of the lawful basis which you are relying on to Process Personal Data, including the legitimate interests pursued by the Company (see section 6 below for more information);
- if you need to rely on Consent and/or need to obtain Explicit Consent for a Processing activity and there are not already agreed procedures in place for doing so (see section 6 below);
- if you are unsure about the retention period for the Personal Data being Processed (see section 10 below);
- if you are unsure about what security or other measures you need to follow to protect Personal Data (see *section* 11 below);
- if there has been a Personal Data Breach (see *section* 11 below);
- if you want to transfer Personal Data outside the EEA (see section 12 below);
- if you need any assistance dealing with any rights invoked by a Data Subject (see section 13);
- if you need any assistance responding to a Subject Access Request (see section 13);

- whenever you are implementing a significant, new or amended Processing activity or system. This is because a DPIA may be required (see section 14 below);
- if you plan to use Personal Data for a purpose which is different to the one which it was collected for (see section 7 below);
- if you have any questions about how data protection law applies to direct marketing (see *section* 14 below); or
- if you need help with any contracts or other matters which require Personal Data to be shared with third parties, including our vendors (see section 14 below).

## 5. Personal data protection principles

In our business, we adhere to the data processing principles set out in the GDPR. All Company Personnel have responsibility for upholding these principles in everything they do.

A list of the principles is set out below. Next to each principle is a reference to the section of this Policy which explains that principle in more detail. Please read each section carefully as they are all equally applicable to how we operate our business. In the future, if you need a refresher of your data protection obligations then this list is a helpful starting point.

### The Principles

***Lawfulness, Fairness and Transparency*** – section 6. Personal Data must be processed lawfully, fairly and in a transparent manner

***Purpose Limitation*** - Section 7. Personal Data must be collected only for specified, explicit and legitimate purposes.

***Data Minimisation –*** section 8 – Personal Data must be adequate, relevant and limited to what is necessary for the purposes for which it is Processed.

***Accuracy*** - Section 9. Personal Data must be accurate and kept up to date.

***Storage Limitation*** - Section 10. Personal Data must not be kept for longer than is necessary to carry out the purposes for which the data was collected.

***Security, Integrity and Confidentiality*** - Section 11. Personal Data must be 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.

***Transfer Limitation*** - Section 12. Personal Data must not be transferred to another country without appropriate safeguards being in place.

***Data Subject's Rights and Requests*** - Section 13. Personal Data must be made available to Data Subjects. Data Subjects must be allowed to exercise certain rights in relation to their Personal Data.

***Accountability*** - Section 14. We are responsible for and must be able to demonstrate compliance with the data protection principles listed above

## 6. Lawfulness, fairness, transparency

**Lawfulness and fairness**

The Company can collect, Process and share Personal Data provided it is done so lawfully and fairly. Under GDPR, Personal Data is Processed lawfully and fairly if it is carried out on one of the grounds listed in Article 6 (for non-sensitive Personal Data only) or Article 9 (for Sensitive Personal Data only).

The following sub-sections list the Company's most-used lawful and fair grounds for processing the Personal Data of customers, third parties and Company Personnel. Underlined terms reflect the wording used in the relevant sections of the GDPR.

**Grounds for Processing customer, supplier, contractor and other third-party data**

Under GDPR, the grounds we most commonly rely upon to justify our lawful and fair Processing of customer, supplier, contractor and other third-party data are as follows:

- Processing is necessary for the performance of a contract with the Data Subject or to take pre-contractual steps at the Data Subject's request. This includes, for example, where we Process a customer's Personal Data in order to provide them with a fee estimate for our services.

- Where the Data Subject contacts us on behalf of a company (e.g. where they are an employee of a business which supply services to us or purchase products from us) then our Processing of the employee's Personal Data (such as their name and email address) is justified on the ground that we have a legitimate interest in doing so,

- because we need to use those details to respond to the Data Subject's queries and to arrange the relevant agreements. To rely on the legitimate interest ground of processing, we have to ensure we do not prejudice the interests or fundamental rights and freedoms of the Data Subjects. This is a balancing act where we must weigh up our business interests against the interests of the Data Subject, such as them wanting to limit how businesses such as ours use their Personal Data. The ICO has helpful guidance on the legitimate interest found for processing which is available at the following URL: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/. If you are looking to justify Processing of Personal Data on the legitimate interest basis and we do not already have established procedures in place for doing so then you should first read the linked ICO Guidance or speak to the Quality and Compliance Manager.
- We also rely on the legitimate interest ground for processing where, for example, we have a legitimate interest in sending marketing material to existing customers or people who have made enquiries about our products and services in the past. This is the case where we are relying on the 'soft opt-in' (please see section 0 below for more information). In this example, the Data Subject's interests and fundamental rights and freedoms are not prejudiced because recipients can opt out of receiving marketing materials at any time (e.g. by clicking 'unsubscribe' in one of our emails).
- We have the Data Subject's Consent. This is usually only required in the context of sending marketing communications where we cannot rely on the soft opt-in/legitimate interest grounds of Processing discussed above. More information about Consent is included in section 0 below.
- The processing is necessary to meet our legal compliance obligations. This includes, for example, keeping proper accounting records.

# Data Protection Policy

**Classification of Data**

For this policy, data is going to be classified into different categories in line with the Data Protection Act and GDPR legislation

Non-sensitive data

Data whose inappropriate use would not adversely affect an individual for example

- Management information reports which do not identify individuals
- Any data which has been made a matter of public record

Sensitive Data

Sensitive data includes

- Any data identified by the Data Protection Act (1988) as personal sensitive data, specifically data relating ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual list offences or alleged offences.
- Data that if lost or stolen would be likely to cause damage or distress to one or more individuals. This includes but it is not limited to human resources data or any information that is not a matter of public record.
- Any data, which may reasonably be expected to be considered sensitive, personal confidential or commercially confidential. For example, data or materials pertaining to existing or planned developments which may be of interest to a competing organisation

Highly Sensitive Data

Data which if used inappropriately may have a significant impact on Beyond Encryption or an individual employee or Beyond Encryption user. In particular employee or user banking details or any other data that is believed could be used for illegal purpose e.g. Identity fraud.

**Grounds for Processing Company Personnel data**

Different grounds for Processing apply to our own staff. We typically process Company Personnel's non-sensitive Personal Data on the grounds that we have a legitimate interest in doing so, in order to carry out our responsibilities as an employer. In certain circumstances we will also have a legal obligation to Process employees' Personal Data during their employment with us.

Where the employee's data is Sensitive Personal Data (such as medical information) then our Processing is justified on additional grounds. These primarily include because:

(a) it is necessary for us to carry out our legal obligations (e.g. to accommodate an employee's requirements if they have a disability);

(b) it is in the public interest to do so (e.g. to carry out equal opportunities monitoring);

(c) it is necessary to assess the working capacity of the employee on health grounds; or

(d) in limited circumstances, because the employee has given their consent.

Further information about how the Company processes the Personal Data of Company Personnel can be found in our employee privacy notice.

**Specifying the legal ground for Processing**

For each Processing activity we carry out, we must identify the legal ground we are relying on. If the legal ground is not already set out in the relevant Privacy Notice then you should make a written record of your ground for processing, notify the Data Subject and consider speaking to the Responsible Person if you have any questions.

**Consent**

As stated in the previous section, a Data Controller must only process Personal Data on the basis of one or more of the lawful grounds set out in the GDPR. One of these grounds is Consent. There are

particular rules in the GDPR about the form Consent has to take for it to be a valid justification for the Processing.

A Data Subject consents to Processing of their Personal Data if they indicate their agreement clearly. This can be done by giving a statement (e.g. saying "I agree" over the telephone) or by another positive action (e.g. ticking a box on a web page). Because Consent requires an affirmative action, silence, pre-ticked boxes or inactivity are unlikely to be acceptable. If a document requests Consent to Data Processing, then the way the Data Subject gives their Consent must be kept separate from other matters in the document. Often this will involve inserting a separate data protection section into the document or webpage because under GDPR the Consent must be 'specific' to the Processing and 'unambiguous'.

Data Subjects have the right to withdraw their consent at any time. If a Data Subject tells us they are withdrawing their consent, then we must process that request promptly. Processing which was justified based on that (now-withdrawn) Consent should be stopped unless another lawful basis for Processing can be identified. If you are uncertain whether we can continue Processing, please speak to the Responsible Person immediately and they can advise you.

For the avoidance of doubt, if we are sending marketing communications based on consent and that consent is withdrawn, we cannot then continue to send marketing communications on the legitimate interest basis by relying on the soft opt-in. Instead, all marketing communications to that person should be stopped unless they instruct us otherwise. Communications which concern their agreement/account with us can still be sent in the usual way.

If we receive a Data Subject's Consent to Process their Personal Data for one purpose then additional consent may be required to Process that Personal Data for another purpose, unless the Data Subject has also agreed to that other purpose. 'Refreshing' consent is necessary because Consent under GDPR is specific to the types of Processing which the Data Subject was told about when they gave the Consent. Data Subjects cannot consent to types of Processing that they are not aware of.

# Data Protection Policy

## Consent to Processing Sensitive Personal Data

Unless we can rely on another legal ground for Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision Making and for data transfers outside of the EEA. Usually we will be relying on another legal basis (so do not require Explicit Consent) to Process most types of Sensitive Data but where Explicit Consent is required, you must send a Privacy Notice to the Data Subject to capture Explicit Consent.

As a business, almost all of our Sensitive Personal Data processing will involve employee information. However, all staff should be mindful of occasions where customers might provide us with Sensitive Personal Data, e.g. if a customer contact discloses that they have a disability. This information should be treated with the utmost confidentiality and you should speak to the Responsible Person if you are uncertain about the grounds on which we are processing that Sensitive Personal Data.

When you obtain Consent, you must keep a record. The Company has a legal obligation to demonstrate compliance with the Consent requirements and these records are one way of ensuring we do this.

## Transparency

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects. The information must be concise, transparent, intelligible, easily accessible, and in clear and plain language. This is to ensure that the Data Subject can easily understand the information. The types of information the Company must provide to Data Subjects depends on whether the Personal Data was received directly from the Data Subjects or from elsewhere (e.g. a from third party).

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR. This information includes identifying the Data Controller, the Responsible Person and stating how and why we will use, Process, disclose, protect and retain their Personal Data. We do this by providing the Data Subject with a Privacy Notice when they first provide us with their Personal Data.

For Company Personnel, full information is contained in the Company's contracts of employment and in Company's employee handbook. For customers, suppliers, contractors and third parties, we provide the relevant information in the form of a Privacy Notice.

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. In practice, this means sending them a copy or link to our relevant Privacy Notice. You must also check that the Personal Data was collected by the third party in accordance with the GDPR. Part of this is ensuring that the Personal Data was collected in contemplation of our proposed Processing of the Personal Data, i.e. it cannot have been collected for another reason and re-purposed without the approval of the Data Subjects. This is discussed further in section 7, below.

## 7. Purpose limitation

Personal Data must be collected only for specified, explicit and legitimate purposes. These purposes are typically set out in our Privacy Notice(s) (for customers and third parties) and in the Company's employment contracts and Employee Handbook (for Company Personnel). If Processing needs to be carried out for a purpose not identified in (as applicable) our Privacy Notices, Company contracts or Employee Handbook then you should send a separate notice to the Data Subject and consider speaking with the Responsible Person if you have any queries.

As a rule, Personal Data must not be Processed in any way which is incompatible with the purpose or purposes which we have told the Data Subject about. If we want to use somebody's Personal Data for a purpose which is new, different or incompatible with the purposes we previously stated to the Data Subject then we will need to inform the Data Subject before we carry out that Processing. Additionally, if we are processing the Personal Data on the basis of Consent then we will need to refresh that consent (please see section 6 and/or speak to the Responsible Person for more information).

## 8. Data minimisation

Personal Data must be adequate, relevant and limited to only what is necessary to carry out the Processing activities for which it was collected.

You may only Process Personal Data where your professional duties require you to do so. You must not Process Personal Data received by the Company for any reason unrelated to your job.

Similarly, you may only collect Personal Data where your professional duties require, you to do so and the amount of information should not exceed the minimum required to carry out the required Processing activities. You should ensure that all collected Personal Data is adequate and relevant for its intended purposes or purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted. This should be done in accordance with any data retention guidelines published by the Company.

## 9. Accuracy

The Personal Data we collect, hold and Process must be accurate. It should also be kept up to date if it is being actively Processed. Everybody who works for the Company 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. As best you can, you must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data (subject to the Company's retention policy, for example where out-of-date Personal Data may need to be kept longer for legal reasons).

## 10. Storage limitation

Personal Data must not be kept for longer than is necessary for the purposes for which the data is processed. The exception to this is where the data is properly Anonymised so that the Data Subject is no longer identifiable.

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

The Company maintains retention policies and procedures to ensure that Personal Data is deleted after a reasonable time has elapsed, depending on the purpose for which it was being held. These retention periods are subject to any lawful requirement that the Company keep the data for a longer period.

Having read and understood the Company's retention policies and procedures, you should take all reasonable steps to destroy or erase from the Company's systems all Personal Data that we no longer require, i.e. because the retention period has been reached and there is no justifiable reason (such as a legal obligation) to keep the information for a longer period. This includes requiring third parties (such as external hosting providers) to delete such data where applicable. The Responsible Person can advise you on best practice if you are uncertain about destroying or erasing stored data.

You should ensure Data Subjects are informed of the period for which data is stored and how that period is determined. This will usually be set out in our Privacy Notice (for customers and third parties) or the Company's employment contracts or Employee Handbook (for Company Personnel).

## 11. Security, integrity and confidentiality

**Protecting Personal Data**

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

We will develop, implement and maintain safeguards appropriate to our size and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and the risks we have identified. These include the use of encryption and Pseudo-anonymisation where applicable. We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data.

All Company Personnel are responsible for protecting the Personal Data we hold. You must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

You must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal

# Data Protection Policy

Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

To comply with GDPR, you must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data. These terms are defined as follows:

- **Confidentiality** means that only people who have a need to know, and are authorised to use the Personal Data, can access it.
- **Integrity** means that Personnel Data is accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users can access the Personal Data when they need it for authorised purposes.

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

## Reporting a Personal Data Breach

The GDPR requires Data Controllers to keep an internal record of all Personal Data Breaches and where a Personal Data Breach results in a high risk to the rights and freedoms of Data Subjects, to notify the applicable regulator (in the UK this is the Information Commissioner's Office) and the Data Subject within certain timeframes.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, **do not attempt to investigate the matter yourself**. **Immediately contact the Responsible Person** or, if they are not available, a senior member of the management team. You should preserve all evidence relating to a potential Personal Data Breach.

## 12. 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 by other countries' tax laws. Personal Data originating in one country is considered to be transferred across borders (and therefore potentially outside of the EEA if the receiving country is not in the EEA also) when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

a) 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. Please speak to the Responsible Person to confirm which countries these are;

b) appropriate safeguards are in place such as binding corporate rules, standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the Responsible Person;

c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or, in some limited cases, for our legitimate interest

The Company does not currently transfer Personal Data outside of the EEA. If your professional duties require you to transfer Personal Data outside of the EEA, **you must speak to the Responsible Person before you do so.**

## 13. Data Subjects' rights and requests

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

- withdraw Consent to Processing at any time (see section 6 for more information);
- receive certain information about the Data Controller's Processing activities;
- request access to their Personal Data that we hold (known as a 'Subject Access Request');
- prevent our use of their Personal Data for direct marketing purposes;
- ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data; See Right to Erasure Policy (ISO 0017)
- restrict Processing in specific circumstances;
- challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which Personal Data is transferred outside of the EEA;
- object to decisions based solely on Automated Processing, including profiling;
- prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and

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

You must verify the identity of an individual requesting data under any of the rights listed above. Do not allow third parties to persuade you into disclosing Personal Data without proper authorisation.

**You must immediately forward any Data Subject request ('subject access request") you receive to the Responsible Person.** You should promptly assist the Responsible Person with the Data subject request if asked to do so.

## 14. Accountability

The Company must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Company is responsible for, and must be able to demonstrate, compliance with the data protection principles.

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

- appointing a suitably qualified Responsible Person (where necessary) and an executive accountable for data privacy;
- implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;
- integrating data protection into internal documents including this Policy and Privacy Notices
- regularly training Company Personnel on the GDPR, this Policy and data protection matters including, for example, Data Subject's rights, Consent, legal bases, DPIA and Personal Data Breaches. The Company must maintain a record of training attendance by Company Personnel; and

- 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.

**Record keeping**

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

You must keep and maintain accurate records of our Processing activities. Certain job roles will have more regular record keeping responsibilities, but all members of staff have responsibility for ensuring the Company is compliant with current data protection law.

The Company's records should include, at a minimum, the name and contact details of the Data Controller and the Responsible Person, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. To create such records, data maps should be created which should include the detail set out above together with appropriate data flows. The Responsible Person shall coordinate the maintenance of these records

**Training and audit**

We are required to ensure all Company Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training.

You must regularly review all the systems and processes under your control to ensure they comply with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

# Data Protection Policy

**Privacy By Design and Data Protection Impact Assessment (DPIA)**

We are required to implement Privacy by Design measures when Processing Personal Data. This involves implementing appropriate technical and organisational measures (like Pseudo-anonymisation) to ensure compliance with data privacy principles.

All Company Personnel have an ongoing responsibility to assess what Privacy by Design measures can be implemented on all programs, systems and procedures that Process Personal Data. Data Protection Impact Assessments (DPIAs) should take into account the following factors:

- the state of the art (e.g. the capability of available technology);
- the cost of implementation
- the nature, scope, context and purposes of Processing; and
- the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

If you have any comments or suggestions about how new Privacy by Design measures might be implemented or how existing measures could be improved, then please pass them on to the Responsible Person.

**Impact assessments when implementing new systems**

You should conduct a DPIA (and discuss your findings with the Responsible Person) when implementing major systems, programs or business processes which involve the Processing of Personal Data. These can include:

- (use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

- Automated Processing including profiling and ADM;
- large scale Processing of Sensitive Data; and
- large scale, systematic monitoring of a publicly accessible area (e.g. by CCTV).

**Impact assessments for high risk processing**

Data controllers are obliged to conduct DPIAs for high risk Processing. The Company does not currently conduct high risk Processing although this will be kept under review by the Responsible Person.

**The DPIA process**

A DPIA must include:

(a) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(b) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(c) an assessment of the risk to individuals; and

(d) the risk mitigation measures in place and demonstration of compliance.

**Automated Processing (including profiling) and Automated Decision Making**

Currently the Company does not undertake any Automated Processing or ADM activities, but this position is kept under review. This section is nevertheless included for completeness pending a future time when the Company may start undertaking Automated Processing or ADM.

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

a) a Data Subject has Explicitly Consented;

b) the Processing is authorised by law; or

c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

We must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

**Direct marketing**

We are subject to certain rules and privacy laws when marketing to our customers (or any third party).

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 processed and followed. If a customer 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 (e.g. that person's email address or telephone number is kept on a 'do not call' list which is checked against the Company's marketing database).

**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.

You may 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.

You may only share the Personal Data we hold with third parties, such as our service providers if:

a) they have a need to know the information for the purposes of providing the contracted services;

b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained

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

d) the transfer complies with any applicable cross border transfer restrictions; and

e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

If you have any doubt whether you are permitted to share Personal Data with a third party, please speak to the Responsible Person before taking any action.

# Data Protection Policy

## 15. Changes to this Policy

We reserve the right to change this Policy at any time without notice to you so please check back regularly to obtain the latest copy of this Policy. We last revised this Policy in October 2018.

This Policy does not override any applicable national data privacy laws and regulations in England and Wales.