# OUR POLICY ON DATA PROTECTION

# (PERSONAL DATA PRIVACY STANDARD)

## How to find your way quickly round this policy



## What's this policy about?

We are committed to making sure that we process personal data in line with the UK General Data Protection Regulation and other relevant UK laws ('data protection laws'). All personal data is protected by safeguards under data protection laws, which impose restrictions on how personal data can be used. We recognise that we need to treat any personal data we process in an appropriate and lawful manner.

This policy (also called our 'Personal Data Privacy Standard') sets out our rules on data protection and how we obtain, handle, process, store, transport and destroy personal data, in compliance with data protection laws.

We expect all Staff to conduct themselves in line with this policy and other guidance we provide. If we share any personal data with third parties, we will make sure they take necessary measures to maintain our commitment to protecting personal data.

## Is this policy part of my contract of employment?

No, and we can change this policy at any time, but if any changes are made, we'll always make you aware of them. We may also vary things like time limits, if we feel we need to.

## Who's covered by this policy?

This policy applies to all employees, directors and other officers, workers and agency workers, volunteers and interns. We also require in any contracts with third parties who may have access to any personal data, such as consultants, contractors or suppliers, that they comply with this policy, and we'll make sure they're given access to a copy. All these people are referred to as '**Staff**' in this policy.

## Who's responsible for this policy?

Our Privacy Officer is responsible for making sure our organisation complies with data protection laws and this policy. Ask your manager if you're not sure who our Privacy Officer is.

If we appoint an official Data Protection Officer, or change the title of our Privacy Officer, we'll make sure you're aware of this.

While we ask all managers to work with the Privacy Officer to make sure this policy is followed, its successful operation also depends on you. Please take the time to read and understand it, and go back to the Privacy Officer or your manager with any questions you may have. Any references to Directors in this policy mean the most senior people within our organisation.

Staff are responsible for complying with this policy and any security safeguards or procedures we put in place, to make sure personal data is protected and secure at all times.

## Staff training

New employees must read and understand this policy as part of their induction. All employees will also receive training covering basic information about confidentiality, data protection and security, and any actions to take if a data breach occurs.

Employees should be aware of consequences they, and we as an organisation, may face if this policy isn't followed.

Staff who are not employees will need to familiarise themselves with this policy and comply with its obligations if they obtain, handle, process, store, transport or destroy personal data on our behalf.

## What kind of data does this policy apply to?

We collect, store and process personal data of our current, past and prospective employees, other staff, suppliers, customers, and any other individuals we communicate with. This information may be held on paper or on a computer or other media.

## What is 'personal data' and 'processing'?

**Personal data** is information that can be used, to identify a living human (who are also called '**data subjects**'). It doesn't need to be 'private' – information that is public knowledge or is about someone's professional life is still personal data. This information can also be factual (such as a name, address or date of birth), or it could be an opinion (such as a performance appraisal). A data subject need not be a UK national or resident.

Truly anonymous information is not considered personal data; however if you can still identify someone from the details, or by combining it with other information that you hold or are likely to get hold of, it will count as personal data.

Some types of data are considered to be particularly sensitive and are categorised as '**special category**' personal data. Because of its sensitive nature, this data can only be processed under strict conditions and may require the explicit consent of the data subject. This type of personal data includes data about a person's:

- racial or ethnic origin,
- political opinions,
- religious or philosophical beliefs ,
- trade union membership,
- physical or mental health ,
- sexual life, and
- sexual orientation.

It can also include genetic data and biometric data (where used for ID purposes).

Any data about an individual's **criminal convictions or offences** is also considered particularly sensitive, and can only be processed under strict conditions and may require the explicit consent of the data subject.

**Processing** is almost any type of activity involving personal data. It includes obtaining, recording or holding personal data, or carrying out any operation or set of operations on personal data, including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Anyone who determines the purpose for processing data, and how this processing is carried out, is a **data controller.** They are also responsible for establishing

practices and policies that follow data protection laws. We are a data controller of all personal data used in our organisation.

**Data processors** are any people or organisations that process personal data for a data controller. In our organisation, our third-party suppliers that handle personal data would be considered our data processors. Please note that our employees are not considered data processors.

## How should personal data be processed?

Data protection laws aren't meant to prevent the processing of personal data, but are there to make sure it's done fairly and without adversely affecting the rights of the data subject. The following principles set out how personal data should be processed.

- **Fairness, lawfulness and transparency.** Personal data should be processed in a lawfully, fair and transparent manner.
- **Purpose limitation.** Personal data should be processed only for specified, explicit and legitimate purposes and in an appropriate way.
- **Data minimisation.** Only personal data that is adequate, relevant and necessary for the overarching purpose can be processed.
- **Accuracy.** Personal data must be accurate and kept up to date.
- **Storage limitation.** Personal data should not be kept longer than is necessary to fulfil the purpose for processing.
- **Security, integrity and confidentiality.** Technical and organisational measures must be in place to protect against unauthorised or unlawful processing, and against accidental loss, destruction or damage of the personal data.
- **Transfer limitation.** Personal data should not be transferred to another country without appropriate safeguards in place.
- **Data subject rights and requests.** Individuals should be allowed to exercise their rights in relation to their personal data, and personal data about them should be made available to individuals who request it.
- **Accountability.** We're responsible for demonstrating our compliance with the data protection principles listed above.

## How do we justify processing personal data?

When we process personal data, we must have a specific purpose for processing personal data and a lawful basis for doing so, which could be:

- for the performance of a **contract** (such as an employment contract),
- to comply with a **legal obligation**,
- it's in the **vital interest** of an individual to protect their life,
- the processing is necessary for us to perform a task in the **public interest**,
- it's in our, or a third party's, **legitimate interest** to process personal data for the specified purpose which doesn't override the rights and freedoms of an individual, or

- where the data subject has given explicit **consent**.

As data controller, we will only process personal data on the basis of one or more of these lawful bases.

In relation to consent, please be aware of the following additional guidelines.

- Consent must be freely given, specific, informed and unambiguous from the data subject.
- They must be able to easily withdraw consent at any time, and we must promptly honour their withdrawal.
- Special category and criminal conviction personal data can only be processed with the explicit consent of the data subject, unless we can rely on one or more of the other lawful bases set out above.

## How we will process personal data

### a) We'll be transparent

We'll provide all required, detailed and specific information to data subjects about how their personal data is collected and used. This will be done by providing a clear privacy notice which is concise, transparent, intelligible, easily accessible and in clear and plain language. Individuals will be told:

- who the data controller is (for example, as your employer, we are the data controller of HR personal data),
- who the data controller's representative is (for example, our Privacy Officer),
- what data we collect from them,
- the purpose for using and processing their data,
- our legal basis for doing so,
- who we share their data with,
- how we protect their data, and
- how long we'll keep their personal data.

### b) We'll have a specific purpose

Personal data can only be processed for a specified, explicit and legitimate purpose, which should be included in the privacy notice we send to data subjects. This means that personal data cannot be collected for one purpose and then used for another. If the purpose for processing their personal data changes, the data subject must be informed through a new or updated privacy notice before the processing begins.

### c) We'll only collect data we need

Only personal data that is relevant and necessary for the specified purpose should be collected.

### d) We'll make sure personal data is accurate

Personal data will be checked for accuracy and completeness when we first collect it, and at regular intervals afterwards to make sure it's kept up to date. We'll destroy or update any inaccurate or out-of-date personal data.

### e) We'll only keep data we need

Personal data shouldn't be kept longer than is necessary to carry out the specified purpose. This means that personal data will be destroyed or erased from our systems when it's no longer required, in accordance with our Data Retention Policy.

### f) We'll keep a record

We'll keep full and accurate records of all our personal data processing activities.

## How do we protect the personal data we hold?

We'll make sure that personal data is secured using appropriate technical and organisational measures to prevent any unauthorised or unlawful processing, and against accidental loss, destruction or damage. These measures will be appropriate to our size, scope and business, our available resources and the amount of personal data we hold. They will be in place from the point of our collection of personal data to the point of its destruction.

These measures can include:

- the encryption of personal data or its anonymisation or pseudonymisation (which is replacing identifying information with artificial information so the data subject can't be identified without using additional information that's kept separately and securely),
- making sure anyone who's authorised to use personal data keeps it confidential,
- maintaining the integrity of the personal data so it's accurate and suitable for the processing purpose,
- making sure the personal data is available to any authorised users who need access, and
- a process for regularly testing, assessing and evaluating these measures to ensure the security of processing.

Data subjects can apply to the courts for compensation if they suffer any damage from our loss of their personal data.

## What happens if there's a data breach?

A **data breach** is any act or omission which compromises the security, confidentiality, integrity or availability of personal data. This could include a problem with our (or a third party's) security safeguards that causes personal data to be lost or accidentally shared with unauthorised people.

If a data breach occurs and is likely to result in a risk to the rights and freedoms of an individual, we'll report it to the Information Commissioner's Office within 72 hours of us becoming aware of the breach. We may report it in more than one instalment.

Where a data breach is likely to result in a high risk to the rights and freedoms of individuals, we'll also directly inform them about the breach and, if the breach is serious, we may also notify the public as soon as possible.

If you know or suspect that a data breach has occurred, contact the Privacy Officer, your manager or a Director immediately, and preserve all evidence relating to the potential data breach. Please don't investigate the matter yourself.

For more information on our data breach procedure, please read Our Policy on Personal Data Breaches.

## Can we transfer data internationally?

Data protection laws restrict transferring personal data to countries outside the UK. This is to make sure that the level of protection given to individuals by the UK GDPR is not undermined.

We can only transfer personal data outside the UK if one of the following conditions applies:

- the UK has officially confirmed that the country receiving the personal data has an adequate level of protection for data subjects' rights and freedoms,
- appropriate safeguards are in place, such as binding corporate rules, standard contractual clauses approved for use in the UK, or an approved code of conduct or a certification mechanism,
- the individual has provided explicit consent to the transfer after being informed of any potential risks, or
- the transfer is necessary for another reason described in the UK GDPR, such as:
  - performing a contract between us and the individual,
  - it's in the public's interest,
  - to establish, exercise or defend legal claims,
  - to protect the vital interests of the individual if they are physically or legally incapable of giving consent, or
  - in some cases, for our legitimate interests.

## Data subjects' rights and requests

All individuals retain rights over how their personal data is handled under data protection laws. These include the following rights.

- The right to be informed about the processing of their personal data.
- The right of access to their own personal data.
- The right for any inaccuracies to be corrected (or 'rectification').
- The right to have information deleted (or 'erasure').
- The right to restrict the processing of their personal data.
- The right to data portability.
- The right to object to the processing of their personal data.

- The right to regulate any automated decision-making or profiling of their personal data.
- The right to withdraw their consent (if consent is the only legal basis for processing their personal data).
- The right to be notified of a data breach, if it's likely to result in a high risk to their rights and freedoms.
- The right to complain to the Information Commissioner's Office or other supervisory authority.

We may receive a written, formal request from a data subject for details asking what personal data we hold about them (also called a '**Data Subject Access Request**'). If you receive this type of written request, please forward it to your manager immediately.

## Automated processing and decision-making

We must follow further, specific rules to protect data subjects' rights and freedoms if we process their personal data using any automated processing (including profiling) or automated decision-making ('**ADM**').

We'll provide you with separate guidelines to follow, if need be, where we engage in profiling or using ADM in a data processing activity.

## Direct marketing

We must follow additional rules and privacy laws if we process any personal data when marketing to our customers.

We'll provide you with separate guidelines to follow, if need be, where you're using personal data for direct marketing purposes.

## Breaches of this policy

If you feel that this policy hasn't been followed in respect of your own personal data or that of others, please raise this with the Privacy Officer, your manager or a Director.

Failure to follow this policy and other rules on data security will be taken seriously and may be dealt with under our Disciplinary Procedure.

## And that's it... for now

We understand that things change, so we'll continue to review the effectiveness of this policy and make sure it's achieving its objectives.