

**GDPR TEMPLATE:**

**DATA PROTECTION POLICY**

**Points to note**

* Before using this template Data Protection Policy, it is essential that you read these ‘Points to note’, together with the separate document, ‘Make UK Essential GDPR Templates for HR – Points to note’, which provides important information applicable to all of the template documents, including the Data Protection Policy.
* This template Data Protection Policy focuses on an organisation’s obligations as a controller under data protection law. It is to be provided to all Employees (as defined in the body of the document), and aims to do the following:
  + Set out a summary of the employer’s approach to data protection compliance with regard to the processing of personal data.
  + Tell Employees what the employer expects of them and what their obligations are when they handle personal data in the course of their job duties. These expectations and obligations apply to any personal data that the Employees process in the course of carrying out their job duties, regardless of whether the data is about other Employees, customers, suppliers or other third parties.
  + Together with the Data Retention Process and the Record of Processing, operate as an ‘appropriate policy document’, which explains the procedures you follow to ensure compliance with the GDPR, in relation to certain uses of special category data. If you intend to use these documents as your appropriate policy document, it is especially important that you assess what you do in practice to comply with the GDPR and ensure that the content of these documents is an accurate reflection of your practices in respect of the processing of special category data.
  + Satisfy the particular obligation to *demonstrate* compliance with data protection law (also referred to as the ‘accountability’ principle).
  + Be an organisational measure that helps the employer to ensure data protection compliance by design and by default.
* This Policy only sets out the broad principles of data protection compliance. Further details of how to handle personal data in particular roles should be given separately to relevant Employees. In other words, certain Employees will need specific instructions in relation to the data processing activities that they are responsible for – and this Policy refers to such instructions where appropriate.
* Rather than simply describing the law, this Policy is intended to provide Employees with a realistic and practical approach to achieving data protection compliance objectives. It works on the basic assumption that, provided Employees are acting within the normal remit of their role and following lawful instructions from their employer, their routine handling of personal data will be compliant with data protection law under the employer’s compliance procedures. In contrast, it highlights the need to contact the appropriate person/team responsible for data protection if Employees have any concerns regarding the handling of personal data or where they are undertaking new projects or processing activities which may not have previously been checked by the employer for data protection compliance.
* There is no ‘one size fits all’ for a Data Protection Policy. Organisations will need to adapt and customise this template to the particular circumstances of their business; the Policy must reflect reality. In addition, whilst this Policy applies to the use of all personal data, some of the examples and guidance are focused on the use of Employee data since this is something Employees are likely to be dealing with and therefore need to understand, in order to implement the policy in practice. Organisations should consider adapting and expanding the examples and guidance to cover other standard uses of data, as relevant to their specific business.
* This Policy focuses on requirements under the GDPR. Organisations may also wish to add other particular provisions depending on the nature of their business, e.g. to cover obligations under ePrivacy Regulations such as those relating to direct marketing and cookies.
* We have presented the Policy in a text/print-out format. However, depending on the organisation’s technological capabilities, it could be presented in a more user friendly form, e.g. online on your company intranet, etc. You may also wish to add features to assist with navigation, such as an index and links to and between specific sections.
* Whether you are introducing a Data Protection Policy for the first time, or updating your existing Policy, when presenting this document to Employees and implementing it in your organisation, you must make clear in your communications that this document replaces any previous policy that they may have been given in the past. This could be done, e.g. in cover emails sending Employees links to the Policy on the intranet, and/or as cover sheets to a hard copy Policy that you distribute to all Employees.
* In order to demonstrate your compliance with the GDPR, you will need to keep a record showing that you have distributed the Policy to all Employees. If you send out a communication by email, the sent emails could serve as your record. If you provide Employees with hard copies, you will need to create a record – this could be as simple as keeping a list of Employee names together with a note of the date on which they were given / sent each of the documents.
* Note also that this Policy should not be presented to Employees in isolation, but should be accompanied by appropriate training – see ‘Make UK Essential GDPR Templates for HR – Points to note’ for further details. You should also keep a record of associated training and awareness activities attended by each Employee and relating to this Policy.

**Customisation**

You should customise all relevant parts of the Policy. However, the following table indicates which sections may need particular tailoring and explains why certain sections have been drafted in a particular way.

|  |  |
| --- | --- |
| **Section of Policy** | **Points to note** |
| Introduction | Clearly, employers should only include reference to other policies that they actually have.  We state that the company is a controller of personal data. This will be the case for all businesses in respect of most personal data that they handle, and this Policy does not cover personal data in respect of which a company is a processor rather than a controller. |
| Who does the Policy apply to? | We suggest that this Policy applies to the entire workforce, regardless of the particular contractual arrangement. This is similar to a harassment or equality policy. The list of individuals who are covered by the defined term “Employee” should be customised to reflect the categories of individuals who work for the company. |
| What is personal data? | This section is unlikely to need customisation. Note that business data counts as personal data. |
| 1. Process personal data in a fair, lawful and transparent manner | Consent is listed in the Policy as one of the legal grounds for processing personal data because it is appropriate for some types of processing, such as sending direct marketing communications. However, consent is rarely an appropriate legal ground for processing personal data in the employment relationship because of the view that consent cannot be freely given, due to the imbalance in power between the parties.  Often, employers will rely on the ‘legitimate interests’ legal ground for processing, i.e. that the processing is necessary in the employer’s or a third party’s legitimate interests – although this must be balanced against the interests and rights of the data subject. The ICO recommends that controllers conduct a ‘legitimate interests assessment’ (LIA) to assist with this balancing exercise. A template LIA form is available on the ICO website: <https://ico.org.uk/media/for-organisations/forms/2258435/gdpr-guidance-legitimate-interests-sample-lia-template.docx> |
| 2. Take extra care when handling special category data | We have included criminal offences/convictions here; even though they are not listed as ‘special category data’ in the UK GDPR, similar restrictions apply to them under the DPA 2018. |
| 6. Keep data for no longer than is necessary for the identified purposes | The Policy takes a high level view of retention. It sets out the criteria the employer uses to set retention periods and tells Employees to follow specific retention policies/guidelines/instructions on data retention. For Employee personal data, these instructions are set out in the GDPR Template: Employee Data Retention Process, but companies will need separate processes for other personal data such as customer data, for example. The criteria included in this section match the criteria in the GDPR Template: Employee Privacy Notice and the GDPR Template: Employee Data Retention Process, which deals with HR/Employee data only. If other retention criteria are adopted for other types of personal data, then the company will need to reflect that here. |
| 7. Take appropriate steps to keep personal data secure | This section of the Policy will require customisation and you need to take care over it. This is because a key area of GDPR compliance relates to data security. Also, breaches of security are likely to be the most damaging type of breach for a company, both in terms of reputation and in potential fines/damages. Having clear standards in the Data Protection Policy is an appropriate organisational measure to ensure security, though it will need to work alongside other internal policies and processes. If you already have a security policy, such as an Information Security Policy, you can refer out to this rather than including full details here. Information Security Policies, which are usually ‘owned’ by the IT department, typically cover many aspects of IT security/disaster recovery, but also building security, disposal of paper files, storage of files, etc. Some companies may also have instructions in a Technology and Communications Policy and/or a Home Working Policy. Companies need to check how comprehensive any existing policies are, and HR will need to work with other departments to do this. If there are no comprehensive policies dealing with data security, then this Policy will have to list security measures that are not included elsewhere. In any event, we recommend that you draw attention to particular areas of concern in the ‘What you need to do’ section. Some suggested security measures are included in italics in both the employer obligation and the ‘what you need to do’ sections – but companies will need to tailor these to their own circumstances and expectations. If you don’t currently have an Information Security Policy, you may wish to consider putting one in place. |
| 8. Take extra care when sharing or disclosing personal data | This section deals with sharing personal data both internally and externally. The process of sharing or disclosing – i.e. the transfer of the data – is itself a form of processing. Note too that sharing personal data with a group company counts as external sharing. All companies will need the paragraphs about internal sharing, which appear in the employer obligation section and the ‘what you need to do’ section. The section about external data sharing may need to be tailored to reflect the external sharing that the company actually carries out, by amending or adding to the examples in brackets or potentially adding a new paragraph as appropriate. However, note that the Policy does not require the level of detail that is needed in a privacy notice about data sharing – it should remain ‘high level’, but be consistent with the information about sharing data that is in the company’s main privacy notices given to individuals (whether they be Employees, customers, suppliers, etc.) There are detailed bullet points in the ‘what you need to do’ section, because it is very important that Employees do not disclose personal data in the wrong circumstances, but note the third paragraph – if a particular role involves regular disclosures to third parties, e.g. if you are in HR and you liaise about staffing issues with the parent company, then the Policy assumes that the company has already put any necessary measures in place to ensure that the disclosures will be GDPR compliant. Check this is the case. |
| 9. Do not transfer personal data to another country (or receive it from another country) unless there are appropriate safeguards in place | Since it is written from the perspective of a UK-based company, this Policy focuses primarily on compliance requirements for transfers of personal data out of, rather than into, the UK. However, it also recognises that there may be occasions when third parties in other countries send personal data to the company in the UK.  This section should be included even if you do not currently transfer personal data to third parties outside the UK. This is because Employees need to know that, if a situation arises where they are considering such a transfer, they may need to get guidance from the appropriate person before doing so.  The section assumes that you will already have the necessary arrangements in place for Employees who are transferring personal data outside the UK (or receiving personal data from another country) in the course of their job. Note that the restrictions on transfer of personal data outside the UK also apply to cloud based storage where the cloud/server is based outside the UK.  This section reflects the fact that the UK has now left the EU and that the post-Brexit transition period came to an end on 31 December 2020. It assumes that personal data can flow freely between the UK and the EEA. This is on the basis that:   * the UK Government has recognised the adequacy of data protection provisions in EEA countries, thereby allowing the continued transfer of personal data from the UK to the EEA; and, * with regard to transfers of personal data from the EEA to the UK, on 28 June 2021, the EU Commission formally adopted an adequacy decision in respect of the UK. The adequacy decision is valid for an initial period of four years, after which it can be renewed if the EU Commission is satisfied that the UK continues to provide an adequate level of protection for personal data.   For transfers of personal data from the UK to non-EEA countries, an adequacy decision or a transfer risk assessment and appropriate safeguards are required. For transfers of personal data from non-EEA countries to the UK, measures may be required under the local law of the data exporting country – see ‘Make UK Essential GDPR Templates for HR – Points to note’ for further details. |
| 10. Report any data protection breaches without delay | You will need to tailor this section so that it fits with your actual procedures. Note that the template wording refers to having internal processes for dealing with personal data breaches (and see our GDPR Template: Guide to Handling a Personal Data Breach).  Note that the wording here refers to reporting personal data breaches to the ICO and possibly also to “supervisory authorities in other countries if the breach occurs in or affects individuals in other countries”. This is because a personal data breach affecting individuals in EEA countries will engage the EU GDPR, which also includes a reporting obligation, and data protection laws in other countries outside the EEA may also impose breach reporting requirements if the breach affects individuals in those countries. If you have a lead supervisory authority in the EEA, you would usually report personal data breaches that affect individuals in EEA countries to that authority – and you may wish to tailor the wording in this section to reflect that. (For further information on lead supervisory authorities, see the ‘Points to note’ on our GDPR Template: Guide to Handling a Personal Data Breach.) |
| 11. Automated decision-making | It is likely that many companies will do some automated decision-making – given that the Policy applies to all personal data, not just Employee personal data. You should include this paragraph even if you don’t currently do any automated decision-making, so that Employees know to seek guidance from the appropriate person if they are considering doing it. The template wording includes various options – for companies who do/don’t carry out profiling/automated decision-making in relation to certain categories of data subjects – and should be customised based on what you currently do. |
| Individual rights and requests | If you have any particular polices or processes dealing with these rights (such as our GDPR Template: Guide to Handling Individuals’ Requests to Exercise Data Protection Rights), this section could be customised to refer to these. (Note that we have included the right to withdraw consent, since the Policy deals with all personal data and not just Employee personal data). |
| Training | This section is self-explanatory but should be amended if necessary to ensure that it reflects what the company actually does. |

**Data Protection Policy**

**Introduction**

At [COMPANY], we collect and process ‘personal data’ (see ‘What is personal data?’ below) for business purposes, including employment and HR administration, provision of our services, marketing, and business administration. This includes personal data relating to our staff, customers, suppliers and other third parties.

Compliance with data protection law is essential to ensure that personal data remains safe, our business operations are secure and the rights of individuals are respected. [COMPANY] is a controller under data protection law, meaning it decides how and why it uses personal data.

This Policy explains our procedures for complying with data protection law in relation to personal data. It also sets out your obligations whenever you are processing any personal data in the course of your employment. Failure to comply with your obligations under this Policy could lead to disciplinary action and, in serious cases, it could result in the termination of your employment.

If you routinely handle individuals’ personal data, you will be given specific [training/instructions] regarding data protection procedures in relation to your particular [role/department]. [This/these] [training/instructions] will supplement your obligations as set out in this Policy.

This Policy does not give you any contractual rights. It may be updated at any time.

**Who does this Policy apply to?**

This Policy applies to all [COMPANY] employees, workers, [contractors, agency workers, consultants, interns, volunteers, partners and directors], (together referred to as ‘Employees’ or ‘you’).

**Who is responsible for data protection at [COMPANY]?**

The Board is ultimately responsible for [COMPANY]'s compliance with applicable data protection law. [COMPANY] has appointed a [Data Protection Officer/Data Protection Lead] who is responsible for overseeing, advising [COMPANY] on and administering compliance with, this Policy and data protection law. [*Also briefly describe any other relevant roles, such as Data Protection Champions, Data Protection Team, Department Heads].*

All Employees at [COMPANY] have some responsibility for ensuring that personal data is kept secure and processed in a lawful manner although certain Employees will have particular responsibilities, of which they will be aware and in respect of which they may receive specific instructions.

If you are in any doubt about how you should handle personal data, or if you have any concerns or questions in relation to the operation (or suspected breaches) of this Policy, you should seek advice from the [Data Protection Lead/Data Protection Officer/Data Protection Team] [*insert contact details*].

**Why is data protection compliance important?**

Data protection law in the UK is regulated and enforced by the Information Commissioner’s Office (ICO). Failure to comply with data protection law may cause harm to individuals and expose [COMPANY] and, in some cases, individual Employees to serious legal liabilities. These can include criminal offences and fines of up to £17.5million or 4% of total worldwide annual turnover, whichever is higher. In addition, an individual may seek damages from us in the courts if we breach their rights under data protection law. Breaches of data protection law can also lead to serious damage to our brand and reputation.

**What is personal data?**

Personal data means any information relating to any living individual (also known as a ‘data subject’) who can be identified (directly or indirectly), in particular by reference to an identifier (e.g. name, NI number, employee number, email address, physical features). Relevant individuals can include your colleagues, consumers, members of the public, business contacts, etc. Personal data can be factual (e.g. contact details or date of birth), an opinion about a person's actions or behaviour, or information that may otherwise impact on that individual. It can be personal or business-related.

The rules apply to personal data held electronically (e.g. within local or cloud-based computer systems, within emails and other communications) or in structured paper (or other manual) files (e.g. personnel files). The rules also apply to paper records which are intended to form part of a structured paper or electronic systems (such as records awaiting filing).

Data protection law provides additional protection for certain categories of personal data known as **special category data**. This is covered in more detail below in this Policy.

What does ‘processing’ personal data mean?

‘Processing’ personal datameans any activity that involves the use of personal data (e.g. obtaining, recording or holding the data, amending, retrieving, using, disclosing, sharing, erasing or destroying). Note that this includes sending or transferring personal data to third parties, as well as use within [COMPANY].

**Related policies and procedures**

There are other policies which will impact on how you deal with personal data and data protection. The main ones are our [Information Security Policy] [Electronic Communications Policy] [*insert references to other relevant policies*], and we expect you to comply with these where relevant. A copy of all these documents is available [on our intranet at [ ]].

**Data Protection Obligations**

[COMPANY] is responsible for and must be able to demonstrate compliance with data protection law. To ensure that [COMPANY] meets its responsibilities, it is essential that its Employees comply with data protection law and any other [COMPANY] policies, guidelines or instructions relating to personal data when processing personal data in the course of their employment.

We have set out below the key obligations under data protection law and details of how [COMPANY] expects Employees to comply with these requirements.

1. **Process personal data in a fair, lawful and transparent manner**

**Fairness and legal ground for processing**

Data protection law allows us to process personal data only where there is a legal ground which justifies us using the information.

Examples of legal grounds for processing personal data include the following (at least one of these must be satisfied for each processing activity):

* processing is necessary to comply with a legal obligation (e.g. health and safety or tax laws);
* processing is necessary for entering into or performing a contract with the individual (e.g. an Employee's terms and conditions of employment, or a contract for services with an individual customer);
* processing is necessary in [COMPANY’S] or a third party’s legitimate interests (e.g. maintaining records of business activities, monitoring business productivity) although this must be balanced against the interests and rights of the individuals. A 'legitimate interests assessment' (LIA) should generally be undertaken before relying on this basis [(and [COMPANY] uses the ICO’s template LIA for this purpose)]; and
* the individual has provided consent to the processing (e.g. for sending direct marketing communications).

Where consent is relied upon, it must be freely given, specific, informed and unambiguous. To this end, consent should be clearly separated from other matters, and should not be wrapped up within other agreements with the data subject (such as within terms of service). It should also be a genuine option (such that the activity will not take place if consent is not given and will cease if consent is subsequently withdrawn). [COMPANY] must effectively demonstrate that consent has been given.

In line with ICO guidance regarding the employment relationship, [COMPANY] does **not** use consent as a legal ground for processing Employee data unless the data processing activities concerned are genuinely optional.

In most cases, consent is also not required for other standard business activities involving use of customer or supplier data, but it may be needed for activities which are not required to manage the main business relationship, such as some direct marketing activities. Consent should not generally be relied upon for use of Employee data unless the data processing activities are genuinely optional.

[COMPANY] identifies the appropriate legal ground for each of its activities within our separate Records of Processing Activities, and within privacy notices provided to individuals.

**Fairness**

Data protection law also requires [COMPANY] to process personal data fairly. This includes ensuring that we only handle personal data in ways that people would reasonably expect and that we do not use it in ways that have unjustified adverse effects on them.

**Transparency**

Data protection law also requires us to process personal data in a transparent manner by providing individuals with appropriate, clear and concise information about how we process their personal data.

We usually provide individuals with basic information about how we use their data on forms which collect data (such as application forms or website forms), and in longer privacy notices setting out details including: the types of personal data that we hold about them, how we use it, our legal grounds for processing the information, who we might share it with and how long we keep it for. For example, we provide information about our processing of Employees’ personal data in [the [COMPANY] Employee Privacy Notice].

We supplement these notices, where appropriate, with reminders or additional information at the time particular processing activities take place or become relevant for an individual (for example when they sign up for a new service or event).

*What you need to do:*

You should process personal data only in accordance with your lawful job duties and [COMPANY]’s standard procedures and instructions. By doing this, ordinarily, you will be processing personal data fairly and lawfully.

The standard privacy notices and statements that we issue, for example, to Employees, customers and the public, should normally be sufficient to ensure that you are processing personal data transparently, i.e. that individuals have appropriate information about how you are handling their personal data in the course of your employment. However, you should consider whether reminders or additional information may be appropriate at the time particular processing activities take place. This is particularly important if you think that individuals may need further assistance to understand clearly how their data will be used as part of such activities. Any requested additional information or clarifications should be discussed with the [Data Protection Lead/Data Protection Officer/Data Protection Team].

Any new forms which collect personal data and any proposed consent wording must be approved in advance by the [Data Protection Lead/Data Protection Officer/Data Protection Team].

If you have any concerns about the legal ground for processing personal data or the fairness of processing, or if you are unsure whether individuals have been provided with appropriate information (in particular in relation to any new processing activities), please check with the [Data Protection Lead/Data Protection Officer/Data Protection Team].

1. **Take extra care when handling special category data**

Some categories of personal data are ‘special’ because they are particularly sensitive and inappropriate use of such data is likely to have a significant negative impact on the data subjects. ‘Special category data’ is personal data about an individual’s:

* racial or ethnic origin;
* political opinions;
* religious or philosophical beliefs;
* trade union membership;
* physical or mental health;
* sex life or sexual orientation;
* biometrics (if used for identification purposes) or genetics; and/or
* criminal offences or convictions.

Where special category personal data is concerned, data protection law requires us to have (as well as one of the legal grounds described in section 1), an additional legal ground to justify using this sensitive information. The appropriate legal ground will depend on the circumstances.

Additional legal grounds for processing special category data include the following. Those marked with an asterisk (\*) would be particularly relevant to processing Employees’ special category personal data:

* processing is necessary to comply with a legal obligation/exercise a legal right in relation to employment\*;
* processing is necessary to carry out equal opportunities monitoring in relation to racial or ethnic origin, religious beliefs, health or sexual orientation\*;
* processing is necessary for exercising, establishing or defending legal claims\*;
* processing is necessary for preventing or detecting unlawful acts; or
* the individual has given their explicit consent. (As well as the requirements for consent outlined in section 1 above, this requires an express statement from the individual that their special category of data may be used for the intended purposes.)

[COMPANY]’s Record of Processing sets out the types of special category data that we process and lists the applicable additional legal grounds for such processing. A copy of the Record of Processing is available from the [Data Protection Lead/Data Protection Officer/Data Protection Team].

Of course, all of the obligations under data protection law that we refer to in this Policy are of particular importance when we process special category data. [COMPANY] has carried out an assessment of its processing of such data in order to ensure that we comply with these obligations in practice.

*What you need to do:*

If you are handling special category personal data in the course of your employment, you need to take extra care because there are more onerous requirements regarding compliance with data protection law.

In particular, you must ensure that:

* any processing activities are strictly in accordance with your lawful job duties and [COMPANY] instructions;
* there are appropriate legal grounds for processing the data (both basic grounds under section 1 and additional grounds under this section 2) which have been assessed for your specific activities;
* individuals have received adequate information regarding how their data is being handled. In some cases, an existing privacy notice may need to be supplemented with more specific information regarding special category data (e.g. when [COMPANY] is managing sickness absence and/or making adjustments to job duties for Employees with disabilities or serious illness, we may provide additional privacy notice information to supplement the Employee Privacy Notice);
* you apply additional security and confidentiality measures, taking into account that the impact on individuals of loss or misuse of their special category data may be greater than with other types of data. See also section 7 below;
* if you are relying on consent as a legal ground for processing, you obtain advance approval of any consent wording from the [Data Protection Lead/Data Protection Officer/Data Protection Team].
* *[Insert details of any additional actions you require Employees to take when handling special category data where your special category legal ground for processing requires an appropriate policy document (e.g. where processing is necessary to comply with a legal obligation or exercise a legal right in relation to employment, or for the purposes of equal opportunities monitoring).]*

If you are routinely handling special category data as part of the requirements of your role and job duties, [COMPANY] will ordinarily have put in place procedures which ensure that your processing activities satisfy these requirements.

However, if alternative circumstances apply (e.g. you are involved in a new project or updating an existing system which involves new types of processing of special category data), please contact the [Data Protection Lead/Data Protection Officer/Data Protection Team] to ensure that the correct compliance procedures are followed.

Similarly, if you are unsure or have any concerns over the legal grounds that apply when you are processing special category data, the fairness of the processing, or the appropriate information to be provided to individuals, please get in touch with the [Data Protection Lead/Data Protection Officer/Data Protection Team].

1. **Only process personal data for specified, explicit and legitimate purposes**

[COMPANY] will only process personal data in accordance with our legitimate purposes to carry out our business operations and to administer employment and other business relationships.

We do not process personal data for different purposes from those for which we originally collected it, unless the new purposes are compatible with the original purposes, to be assessed on a case by case basis taking into account the ICO guidance. We ensure that individuals are properly informed about any new purposes for processing.

*What you need to do:*

You must only use the personal data that you process in the course of your duties for [COMPANY]’s legitimate and authorised purposes, about which individuals have been informed. You must not process personal data for any purposes which are unrelated to your job duties.

Processing personal data for any incompatible or unauthorised purposes could result in a breach of data protection law (e.g. using the company contacts database to find out a colleague’s home address for private, non-work related purposes). This may have potentially damaging consequences for all parties concerned, including disciplinary action against you.

If you find that you need to process personal data for different purposes from those for which it was originally collected, you should contact the [Data Protection Lead/ Data Protection Officer/Data Protection Team] before going ahead with processing the data for that additional purpose.

If you are unsure about whether a particular use of personal data as part of your role is within the scope of legitimate and authorised purposes, you should contact the [Data Protection Lead/Data Protection Officer/Data Protection Team] before going ahead with processing the data for the additional purpose.

1. **Make sure that personal data is adequate, relevant and limited to what is necessary for the legitimate purposes**

Data protection law requires us to ensure that, when we process personal data, it is adequate, relevant to our purposes and limited to what is necessary for those purposes (also known as ‘data minimisation’). In other words, we ask for and use the information we need for our legitimate business purposes, but we won’t ask for or use more information than we need in order to carry out those activities.

*What you need to do:*

You should try to ensure that you only collect, record and use the personal data that you actually need for [COMPANY]'s legitimate and authorised purposes within the scope of your role. You must ensure, however, that you have sufficient personal data to be able to use it fairly for the specified purposes and to take into account all relevant details.

If you are creating forms that collect personal data, you should be able to justify why each specific category of data is being requested or recorded. Consider whether less information, or less specific information, could be recorded to achieve the same purpose.

You should only access information relevant to your role.

You should not create unnecessary copies of personal data.

You must also comply with [COMPANY]’s instructions about data retention and storage, ensuring that personal data is only kept for as long as it is needed for any intended purpose.

1. **Keep personal data accurate and (where necessary) up-to-date**

[COMPANY] must take steps to ensure that personal data is accurate and (where necessary) kept up-to-date. For example, we request that Employees provide us with any change in contact details or personal information via [*insert details of relevant forms or HR portals*]. We also take care that decisions impacting individuals are based on accurate and up-to-date information.

*What you need to do:*

When you process individuals’ personal data in the course of your employment, you must make reasonable efforts to check that the data is accurate and, where necessary, keep the relevant information updated.

When collecting any personal data, try to confirm its accuracy at the outset. If you are unclear on any detail, seek to clarify it directly with the individual. If you subsequently discover any inaccuracies in the personal data that you are handling, these need to be corrected or deleted without delay.

You should limit the number of copies of personal data which are held, to avoid the risk that duplicate copies are not updated and become out of sync. Where possible, you should work from and update a single central copy where possible (in accordance with standard [COMPANY] procedures on retention and storage of records).

1. **Keep personal data for no longer than is necessary for the identified purposes**

Records containing personal data should only be kept for as long as they are needed for the identified purposes. [COMPANY] has in place the following data retention, storage and deletion policies and internal processes/guidelines regarding various types of company records and information that contain personal data, to which you will have access where relevant to your job role:

* Employee Data Retention Process
* [*insert details of other applicable retention and deletion policies, processes and guidelines*].

We take appropriate steps to retain personal data only for so long as is necessary, taking into account the following criteria:

* the amount, nature, and sensitivity of the personal data;
* the risk of harm from unauthorised use or disclosure;
* the purposes for which we process the personal data and how long we need the particular data to achieve these purposes;
* how long the personal data is likely to remain accurate and up-to-date;
* for how long the personal data might be relevant to possible future legal claims; and
* any applicable legal, accounting, reporting or regulatory requirements that specify how long certain records must be kept.

*What you need to do:*

Please familiarise yourself with our retention policies, processes, guidelines and instructions that are relevant to your job. Ensure that, where it falls within your responsibility, you destroy or erase all information that you no longer require in accordance with these.

If you are not sure what retention guidelines/instructions apply to you in your role, or you are unsure of how to apply them to a particular type or item of personal data, please contact the [Data Protection Lead/Data Protection Officer/Data Protection Team].

1. **Take appropriate steps to keep personal data secure**

Keeping personal data safe and complying with [COMPANY]’s security procedures to protect the confidentiality, integrity, availability and resilience of personal data is a key responsibility for [COMPANY] and its workforce.

[[COMPANY] has an [Information Security Policy], which sets out its organisational and technical security measures to protect information, including personal data] [*OR set out detail of information security measures here or in an Appendix, including physical, technological and organisational controls, e.g. locked filing cabinets, building security, information subject to access controls and passwords, reliability checks on/confidentiality obligations of Employees, encryption of hardware or software, pseudonymisation, anti-virus and network protection, software updates, security testing and incident management, secure disposal of records and equipment, backup and disaster recovery, remote working procedures, protocols on use of technology and data storage, asset registers*].

[[COMPANY] also has a [Technology and Communications Policy] setting out protocols for Employees on use of technology and communications systems, which also help to ensure appropriate security of personal data stored or communicated using such systems.]

We regularly evaluate and test the effectiveness of these measures to ensure the security of our personal data processing activities [as set out in our [Information Security Policy]/as carried out by our information security team].

*What you need to do:*

To assist [COMPANY] in maintaining data security and protecting the confidentiality and integrity of the personal data you handle in the course of your employment, we require you to comply with this Policy[, our Information Security Policy][, our Technology and Communications Policy] and any [COMPANY] instructions regarding the processing and security of personal data. [*Include further detail here to the extent other policies are not in place or if you wish to draw out particular areas of concern*][In particular, we require you to:]

[*Insert details as relevant to your particular security measures. These might include things like:*

* *only access and use personal data relevant to your role for [COMPANY]*
* *save, store and communicate personal data only within or using authorised [COMPANY] information and communications systems. Restrict storage of personal data on personal devices or using personal communications facilities (or BYOD controls)*
* *use password-protected and encrypted software for the transmission and receipt of emails*
* *lock files in a secure cabinet [insert details]*
* *never leave your laptop, other device or any hard copies of documents containing personal data in a public place*
* *take care when observing personal data in hard copy or on-screen that such information is not viewed by anyone who does not have the right to that information, especially if you are viewing the personal data in a public place*
* *when storing data on portable devices such as laptops, smartphones, or USB drives, ensure that the device is encrypted and password protected*
* *ensure that information containing personal data is disposed of securely and permanently, using confidential waste disposal or shredding where necessary*
* *if you come across information containing personal data that you are not meant to have access to, e.g. because a document is left on the printer, or someone misdirects an email, inform the document owner (if you know who this is) and securely delete or dispose of the document*
* *alert [the Data Protection Lead/Data Protection Officer/Data Protection Team] to any personal data breaches immediately (see below for further details about personal data breaches)*
* *ensure that any sharing or disclosure of personal data is permitted on appropriate legal grounds and, where necessary, safeguards are in place (see below for further details of safeguards regarding overseas transfers or if sharing personal data with third party service providers)*]

1. **Take extra care when sharing or disclosing personal data**

The sharing or disclosure of personal data is a type of processing, and therefore all the principles described in this Policy need to be applied.

**Internal data sharing**

[COMPANY] ensures that personal data is only shared internally on a ‘need to know’ basis.

**External data sharing**

We will only share personal data with other third parties (including group entities) where we have a legitimate purpose, and an appropriate legal ground under data protection law which permits us to do so. Commonly, this could include situations where we are legally obliged to provide the information (e.g. to HMRC for tax purposes) or where necessary to perform our contractual duties to individuals (e.g. provision of information to our occupational pension providers). We will ensure that data sharing agreements are put in place if appropriate.

We may appoint third party service providers, for example to provide payroll, data storage or other technology services. Where the service provider handles personal data only on our behalf and under our instructions, they will be a ‘processor’ under data protection law.

[COMPANY] remains responsible for ensuring that its processors comply with data protection lawand this Policy in their handling of personal data. We must assess and apply data protection and information security measures prior to and during the appointment of a processor. The extent of these measures will vary depending on the nature of the activities, but will include appropriate risk assessments and reviews, and contractual obligations (within data processing agreements).

Details of the recipients or categories of recipients of personal data (including processors and other third parties) will be set out in privacy notices as described in section 1 above.

*What you need to do:*

You may only share or disclose the personal data we hold internally with an Employee, agent or representative of [COMPANY] if the recipient has a job-related need to know the information.

You may only disclose the personal data we hold to service providers or other third parties (including group entities) where:

* there is a legitimate purpose and an appropriate legal ground for doing so (e.g. it is necessary for them to process the personal data in order to provide a service to us such as a technology service or payroll, or if we are legally obliged to do so);
* the individuals whose personal data is being shared have been properly informed (e.g. in an appropriate privacy notice);
* [COMPANY] has checked that adequate security and data protection measures are in place to protect the personal data concerned;
* the service provider or other third party has signed up to a written data sharing or data processing agreement that contains the provisions required by data protection law (unless the [Data Protection Lead/Data Protection Officer/Data Protection Team] has determined that this is not required in context); and
* the data sharing complies with any overseas transfer restrictions, if applicable (see section 9 below).

Routine disclosures of personal data to established recipients (e.g. standard technology or payroll providers or group entities) which form a normal and regular part of your role and job duties will ordinarily satisfy the above requirements. You should always ensure you comply with any particular [COMPANY] instructions you are given. However, if you are in any doubt as to whether you can share particular personal data with any established recipient, first contact the [Data Protection Lead/Data Protection Officer/Data Protection Team].

You should not share data with any new external party, nor appoint new technology or service providers (including using new technology to process data) without prior approval of and consultation with the [Data Protection Lead/Data Protection Officer/Data Protection Team], who will assist you to assess whether additional measures or agreements are needed prior to disclosure.

1. **Do not transfer personal data to another country (or receive it from another country) unless there are appropriate safeguards in place**

An overseas transfer of personal data takes place when the data is transmitted or sent to, viewed by, accessed by or otherwise processed by a third party in a different country. This includes the use of technology systems hosted (or with backups) outside the UK. (Other companies in the [COMPANY] group are considered to be third parties for these purposes.). Data protection law restricts personal data transfers to countries outside of the UK, to ensure that the level of data protection afforded to individuals is not compromised (as the laws of such countries may not provide the same level of protection for personal data as within the UK).

To ensure that data protection is not compromised when personal data is transferred to another country, [COMPANY] assesses the risks of any transfer of personal data outside of the UK (taking into account the principles in this Policy) and puts in place appropriate safeguards where required.

[***IF YOU CURRENTLY TRANSFER PERSONAL DATA TO THE EEA (SEE POINTS TO NOTE):*** The UK Government has recognised that data protection laws in countries in the European Economic Area (EEA – this is the European Union plus Norway, Liechtenstein and Iceland) provide an equivalent level of protection for personal data. Accordingly, personal data transfers to countries in the EEA are not restricted.]

[***IF YOU CURRENTLY TRANSFER PERSONAL DATA TO COUNTRIES OUTSIDE THE EEA****:* For transfers of personal data outside the EEA, we currently: *[Insert details of countries to which you transfer personal data, whether there are* *adequacy decisions in place in respect of the particular countries, or – if not – the fact that you have conducted a transfer risk assessments and a statement of what safeguards are in place]*.]

[***IF YOU DO NOT TRANSFER ANY PERSONAL DATA OUTSIDE THE UK****:* We do not currently transfer personal data outside the UK.]

Where [COMPANY] receives personal data from a third party in a different country, that third party may need to put in place particular measures in order to comply with the laws of that country regarding transfers of personal data to the UK. [COMPANY] cooperates with such requests received from third parties in order to provide reasonable assistance to enable them to comply with their data protection obligations.

*What you need to do:*

Where overseas transfers of personal data to or from the UK are a normal part of your role and job duties, [COMPANY]’s current arrangements are likely to provide the required levels of data protection.

However, if you are transferring personal data outside the UK in alternative circumstances (e.g. for new types of processing activities which haven’t previously formed part of your job scope and activities, to organisations in the USA with whom you haven’t previously dealt, or to countries with which you haven’t previously dealt), you should contact the [Data Protection Lead/Data Protection Officer/Data Protection Team] for further guidance before going ahead with the transfer. Similarly, if you are receiving personal data from another country in alternative circumstances, you should contact the [Data Protection Lead/Data Protection Officer/Data Protection Team] for advice.

1. **Report any data protection breaches without delay**

[COMPANY] takes all breaches of data protection law and this Policy very seriously. These can include lost or mislaid equipment or data, use of inaccurate or excessive data, failure to address an individual's rights, accidental sending of data to the wrong person, unauthorised access to, use of or disclosure of data, deliberate attacks on [COMPANY]'s systems or theft of records, and any equivalent breaches by [COMPANY]'s service providers.

Where there has been a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data – known as a ‘personal data breach’ – which poses a risk to the rights and freedoms of individuals, [COMPANY] is required to report it to the ICO without delay and, where feasible, within 72 hours of discovery. (Breaches may also need to be notified to supervisory authorities in other countries if the breach occurs in or affects individuals in other countries). [COMPANY] will take immediate steps to identify, assess and address any such breach, including containing the risks, remedying the breach and, where necessary, notifying the ICO and any other appropriate parties (see below). [[COMPANY] has internal processes for identifying, assessing and addressing personal data breaches].

We also keep an internal record of all personal data breaches regardless of their effect and whether or not we report them to the ICO.

If a personal data breach is likely to result in a high risk to the rights and freedoms of individuals, we will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures we have taken.

*What you need to do:*

If you become aware of or suspect any breach of data protection law or this Policy (including, in particular, any personal data breach as described above), you must report it to the [Data Protection Lead/Data Protection Officer/Data Protection Team] immediately via [*insert contact details*]. This will enable us to ensure that the breach is effectively assessed and addressed, as well as to comply with [COMPANY]’s data breach reporting obligations where applicable. The [Data Protection Lead/Data Protection Officer/Data Protection Team] may also need your assistance to assess and address the breach.

1. **Do not use profiling or automated decision-making unless authorised to do so**

Profiling, or automated decision-making, occurs where an individual’s personal data is processed and evaluated by automated means resulting in an important decision being taken in relation to that individual. This poses particular risks for individuals where a decision is based solely on that profiling or other automated processing.

One example of solely automated decision-making would be using an online psychometric test to automatically reject job applicants who do not meet a minimum pass mark (without any human oversight such as a review of the test results by a recruiting manager).

Data protection law prohibits decision-making based solely on profiling or other automated processing, except in very limited circumstances. In addition, where profiling or other automated decision-making *is* permitted, safeguards must be put in place and we must give individuals the opportunity to express their point of view and challenge the decision. [***EITHER:*** We do not generally conduct profiling or other automated decision-making in respect of [Employees’/customers’/*other specified categories of individuals’*] personal data. ***AND/OR:*** Profiling or other automated decision-making carried out by [COMPANY] in relation to [Employees’/ customers’/*other specified categories of individuals’*] personal data is assessed for compliance with these requirements and appropriate safeguards are implemented on a case by case basis.]

*What you need to do:*

If you conduct profiling or other automated decision-making in the course of your role, you must familiarise yourself with and implement any applicable safeguards.

If you are proposing to undertake any new automated decision-making or profiling activities in the course of your employment, please contact the [Data Protection Lead/Data Protection Officer/Data Protection Team], who will advise you whether it is permitted and about the safeguards you need to put in place.

1. **Integrate data protection into operations**

Data protection law requires [COMPANY] to build data protection considerations and security measures into all of our operations that involve the processing of personal data, particularly at the start of a new project or activity which may impact on the privacy of individuals. This is known as 'data protection by design and by default'.

It involves taking into account various factors including:

* the risks (and their likelihood and severity) posed by the processing for the rights and freedoms of individuals;
* technological capabilities;
* the cost of implementation; and
* the nature, scope, context and purposes of the processing of personal data.

A useful tool for assessing data protection and privacy considerations is a Data Protection Impact Assessment or ‘DPIA’. A DPIA will consider the necessity and proportionality of a processing operation, and assess the risks to individuals and the measures that can be put in place to mitigate those risks. A DPIA must be carried out if a data processing operation is likely to give rise to a high risk to individual rights and freedoms. We consider all new processing operations to determine whether a DPIA is required, or if it would be beneficial to conduct a DPIA even if it is not strictly legally required. If we decide not to conduct a DPIA, we ensure that our reasons for this are appropriately documented.

We also seek to assess data protection risks regularly throughout the lifecycle of any project or activity which involves the use of personal data.

*What you need to do:*

If you are involved in the design or implementation of a new project or activity that involves processing personal data, you must give due consideration to all the principles of data protection and rights of individuals as set out in this Policy.

You must also check whether it is necessary to conduct a DPIA or similar risk or compliance assessment by contacting the [Data Protection Lead/Data Protection Officer/Data Protection Team]. They will also be able to advise you on how we expect you to conduct, or otherwise contribute to, a DPIA or similar risk assessment.

You should assist [the Data Protection Lead/Data Protection Officer/Data Protection Team] with regular reviews of projects or activities to ensure data protection risks continue to be addressed.

**Individual rights and requests**

Under data protection law, individuals have certain rights when it comes to how we handle their personal data. For example, an individual has the following rights:

* **The right to make a ‘subject access request’.** This entitles an individual to receive a copy of the personal data we hold about them, together with information about how and why we process it and other rights which they have (as outlined below).
* **The right to request that we correct incomplete or inaccurate** personal data that we hold about them.
* **The right to withdraw any consent** which they have given.
* **The right to request that we delete or remove** personal data that we hold about them where there is no good reason for us continuing to process it. Individuals also have the right to ask us to delete or remove their personal data where they have exercised their right to object to processing (see below).
* **The right to object to our processing** of their personal data for direct marketing purposes, or where we are relying on our legitimate interests (or those of a third party), where we cannot show a compelling reason to continue the processing.
* **The right to request that we restrict our processing** of their personal data. This enables individuals to ask us to suspend the processing of personal data about them, for example if they want us to establish its accuracy or the reason for processing it.
* **The right to request that we transfer** to them or another party, in a structured format, their personal data which they have provided to us (also known as the right to ‘data portability’). The applicability of this right depends on the legal grounds on which we process it.
* **Rights** **in relation to solely automated decision-making (including profiling),** including the right to voice their opinion, to obtain human intervention in the decision-making, and to contest the decision.

We are required to comply with these rights without undue delay and, in respect of certain rights, within a one month timeframe.

Individuals also have rights to complain to the ICO about and to take action in court to enforce their rights and to seek compensation for damage suffered from any breaches.

*What you need to do:*

If you receive a request from an individual seeking to exercise a right in relation to their personal data, or making an enquiry or complaint about our use of their personal data, you must forward the request, enquiry or complaint to the [Data Protection Lead/Data Protection Officer/Data Protection Team] immediately so that it can be dealt with appropriately and within the applicable time limit. Your assistance may be needed to address and respond to the request, enquiry or complaint.

Once you are aware of an access request, you must not do anything to prevent the individual from receiving information they would be entitled to in response to their request. For example, you must not amend, delete, or hide personal data that relate to the request, unless you would have done this in any event in the absence of a request. If you are unsure, you should contact the [Data Protection Lead/Data Protection Officer/Data Protection Team] before taking any action. Failure to comply with this instruction could lead to disciplinary action (including dismissal) as well as criminal liability.

**Record Keeping**

In order to comply, and demonstrate our compliance, with data protection law, [COMPANY] keeps various records of our data processing activities. These include a Record of Processing which contains: the purposes of processing; categories of data subjects and personal data; our legal grounds for processing; categories of recipients of disclosures of data; information about international data transfers; envisaged retention periods; general descriptions of security measures applied; and certain additional details (including legal grounds) in respect of particular types of processing of special category data.

*What you need to do:*

You must comply with our applicable processes/guidelines and any specific instructions you are given concerning the keeping of records about our processing of personal data.

If you are processing individuals’ personal data in the course of your employment and you collect any new types of personal data or undertake any new types of processing activities, either through the introduction of new systems or technology or by amending existing ones, please inform the [Data Protection Lead/Data Protection Officer/Data Protection Team] so that we are able to keep our records up-to-date.

**Training**

We require all Employees to undergo some basic training to enable them to comply with data protection law and this Policy. Additional training may be required for specific roles and activities involving the use of personal data.

To this end, we provide training as part of our induction process for new joiners to [COMPANY] and operate an ongoing training programme to make sure that Employees’ knowledge and understanding of what is necessary for compliance in the context of their role is up-to-date. Attendance at such training is mandatory and will be recorded.

**Departures from this Policy**

There are some very limited exemptions from data protection law, which may permit departure from aspects of this Policy in certain circumstances.

You will be given specific instructions if any exemptions are relevant to your role.

If you think you should be able to depart from this Policy in any circumstances, you must contact the [Data Protection Lead/Data Protection Officer/Data Protection Team] before taking any action.