# Data Protection Policy

## 1 ABOUT THIS POLICY

1.1 THE COSEC RECRUITMENT COMPANY LIMITED (with company number: 14573305) (**we**, **us** or **our**) use information about people (e.g. clients, candidates, website visitors, employees) when we conduct our business. It is a vital asset which we need to carry out our business activities (e.g. providing our products or services, monitoring our website, paying our staff). It is also important to keep this information safe because it can create risk for those people if it is misused or misplaced (e.g. identity fraud).

1.2 The law formally recognises the value and risk of using people's information by creating obligations on organisations that use or access it and granting rights to the individuals that it relates to. This type of law is called **data protection law**. In the UK, it includes the UK GDPR (as defined in section 3(10) of the Data Protection Act 2018, and supplemented by section 205(4)) and the Data Protection Act 2018.

1.3 This policy sets out:

a. what our obligations are under data protection law;
b. what to do if we want to use people's information in a new way;
c. when and how we can share people's information with others;
d. what records we need to keep as evidence that we are fulfilling our obligations;
e. other policies you need to be familiar with.

1.4 This policy applies to all members of THE COSEC RECRUITMENT COMPANY LIMITED's staff: whether you have an employment contract with us or work for us in some other capacity (e.g. contractor, work experience), you must comply with this policy.

1.5 The Information Commissioner's Office (**ICO**) is the UK data protection regulator and is responsible for checking that businesses comply with data protection law.

1.6 The ICO handles complaints and can fine, or take enforcement action against, businesses that do not fulfil their data protection obligations. Failure to comply with data protection obligations can also impact companies' brands and reputations.

1.7 Laura Higgins is our Data Protection Lead and is responsible for advising and monitoring how we use personal data in our business practice. Our directors are responsible for making (and providing adequate resources to implement) any decisions, including whether to report a breach to the ICO.

1.8 From time to time, we may have contracts with third parties (e.g. customers, suppliers) which contain data protection clauses. Contracts can be enforced by parties and ultimately by the courts if there is a disagreement, so it is important that we have policies in place to comply with our obligations.

1.9 Our employment (and equivalent) contracts require our staff to comply with this policy and failure to follow this policy may be a disciplinary matter.

## 2 THE KEY CONCEPTS

2.1 **You must be able to recognise language used in data protection law.** Data protection law uses specific definitions, and you must be able to recognise these definitions so you know what action you need to take (even if that action is referring the matter to the person responsible for data protection):

- **Personal Data:** any information which does (or could be used to) identify a living person. It does not matter whether their information is kept digitally or in hard-copy, or whether it is in writing or some other format (e.g. CCTV footage, photographs). Examples of personal data include: name, email address, postal address, IP address, cookies information, health data and data relating to criminal convictions.
- **Processing:** any action done to personal data - ranging from actively using or analysing the information to simply having access to or storing the information. It even includes deleting information.
- **Data Subject:** the living person who is (or could be) identified by the information.
- **Controller:** the organisation that makes decisions about what and why information is being collected about individuals. For example, THE COSEC RECRUITMENT COMPANY LIMITED will be the controller of personal data relating to our employees.
- **Processor:** an organisation that carries out a task for the Controller which requires them to process personal data. They must follow the instructions they receive from the Controller and there must be a contract in place before they can begin any processing.
- **Lawful Grounds:** a justification that allows an organisation to process personal data. An organisation will be breaking the law if it is not meeting one of the six permitted justifications under data protection laws. We (as a business) must always be able to identify which Lawful Ground we are relying on whenever we process personal data.

## 3 PRINCIPLES OF DATA PROTECTION LAW

3.1 **You must be aware of the 7 principles of data protection law.** Data protection law sets very few specific rules to follow. Instead, the law requires us to consider whether the way we use personal data is in line with 7 principles. It is our responsibility (when we are the Controller) to decide how we achieve the principles. The directors will make the final decision on what action the business can take but you should be aware of the principles so you understand why you are (or are not) able to use personal data in a certain way.

3.2 The 7 principles require us to:

I. **Use personal data in a lawful, fair and transparent way:** We must make sure we know which of the six Lawful Grounds we are relying on (see section below) and how the Data Subject can find out how their information is being used.

II. **Only collect personal data for a specific, explicit and legitimate purpose (purpose limitation):** We must be clear about why we want to use the information and record our decision. We must have a good reason before we begin to collect information about people.

III. **Collect the least amount of personal data we need to achieve our aim (data minimisation):** We must always identify the types of information we plan to collect and decide whether it is necessary to have that information to achieve our aim. If it is not necessary, we should not collect the information at all.

IV. **Make sure personal data is accurate:** We must have processes which ensure we record information correctly and that we can amend it if we later find out there was a mistake.

V. **Only keep personal data for as long as we need it (storage limitation):** We must only keep information whilst we need it to achieve our aim. Sometimes the law requires us to keep information

for a specific amount of time. If we are the Controller, it is our responsibility to decide how long to keep information for and why. We must record our decision. If we are the Processor, we should ask the Controller how long they want us to keep the information for.

VI. **Keep personal data safe (by ensuring its security, integrity and confidentiality):** We must use appropriate technical (e.g. anti-virus, passwords) and organisational (e.g. staff training and working practices) to protect information.

VII. **Demonstrate that we process personal data properly (accountability):** We have compliance documents to record how we use personal data, who we share it with and how we made our decision. We maintain these documents and update them whenever we collect, use or access personal data in a new way or for a new reason.

## 4 USING PERSONAL DATA IN A LAWFUL, FAIR AND TRANSPARENT WAY

4.1 **You must only access or use Personal Data once a Lawful Grounds has been identified (otherwise you are acting illegally).** Whenever we require you to use Personal Data as part of your role, we must ensure that we have identified and met the criteria for one of the six Lawful Grounds set out below. If you do not think there is a valid Lawful Ground for the way that you are using or accessing Personal Data, please speak with our Data Protection Lead to confirm you are able to proceed. We can only use Personal Data to:

(a) **Perform a contract (with the Data Subject):** You can use or access personal data where this is required to carry out a contract (e.g. you need contact details to post a product to the correct address and their financial details to request payment for the product). This Lawful Ground is not valid where we have a contract with another organisation (see instead Legitimate Interest).

(b) **Comply with a legal obligation:** You can use or access personal data where the law requires you to (e.g. reviewing identity documents for right to work checks).

(c) **Prevent risk to life of the Data Subject or another person (vital interests):** You can use personal data where a person's life is at risk. It is unlikely that you would need to use information in this way as part of your role (e.g. emergency contact on HR records, sharing medical information with an attending paramedic).

(d) **Pursue a justifiable commercial aim (legitimate interest):** You can use personal data to help us pursue a legitimate business aim (e.g. increase brand awareness, perform contracts with other organisations, defend legal claims). But you can only do this where the benefits of doing so would not outweigh the risks to the Data Subject. If you are not sure if we have a legitimate interest, whether you can rely on this Lawful Ground, or you receive a question or complaint about the way we use personal data to pursue a commercial aim, you should let our Data Protection Lead know as soon as possible. Where this Lawful Ground is being relied upon, a legitimate interests assessment should be carried out (see *Compliance Records* section below).

(e) **It is part of a public task (public interest):** the processing is necessary to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

(f) **Do the activity that the Data Subject has given their permission (consent) for:** You can use personal data where the individual has stated that they are happy for us to use their information for a specific activity. We only rely on consent for some activities, and we keep a clear record of who has given their consent (permission) and what activity they have given their permission for.

4.2 **You must correctly obtain and record consent (and respect when a Data Subject changes their mind).** Where we intend to use consent as the Lawful Ground for a business activity, it is only valid if the consent is:

- **Specific** (related to a clearly defined activity or purpose);
- **Informed** (explained in a way that the Data Subject understands);
- **Unambiguous and given by a clear affirmative action** (you must not design or use forms with pre-ticked boxes. You must not use a person's information if they have not responded);
- **Separate from other contractual terms** given to the Data Subject;
- **Freely and genuinely given** (it is not appropriate to use consent as a Lawful Grounds where the relationship we have with them could pressure them into accepting, e.g. employer-employee relationship. We cannot refuse to provide our product or service to someone who does not want to provide permission to another activity, e.g. marketing).

4.3 If your role requires you to draft consent wording or obtain consent from individuals, you must always give them the option to change their mind (at the time and at a later date) and withdraw their consent.

4.4 Any marketing communications we send to individuals must include a link which allows the recipient to unsubscribe (this is not mandatory for communications sent to recipients which are businesses).

4.5 **You must be able to direct Data Subjects to the relevant privacy notice.** Individuals have the right to know how their personal data is used by us. We publish privacy notices to explain what information we collect, how we use it and who we share it with. You must be able to direct an individual to the relevant privacy notice (this may be different if depending on what relationship they have with us, e.g. if they are a customer or a member of staff).

4.6 **You must have an additional lawful basis to process any special category data.** Data protection laws treat certain types of personal data as sensitive and requires additional safeguards in place for that data to be processed (known as **special category data**). This includes health data, data relating to religious beliefs, data relating to sexual orientation, biometric and genetic data, data revealing racial or ethnic origin and data revealing trade union membership. Before processing any special category data, you should speak to Data Protection Lead to find out if any additional condition for processing can be relied upon (in addition to one of the Lawful Grounds above).

## 5 USING PERSONAL DATA FOR A SPECIFIC, EXPLICIT AND LEGITIMATE PURPOSE (PURPOSE LIMITATION)

5.1 **You must conduct a due diligence exercise before using personal data for a new purpose.** The Directors decide the purposes for which we use personal data and keep an up-to-date record of the purposes (in the **Record of Processing Activities**, see *Compliance Records* section below). We encourage innovation and new ideas but we also make sure that we consider the impact on Data Subjects before approving new projects or business practices. You must get approval from our Data Protection Lead and complete a **data protection impact assessment** (a specific type of risk assessment document) where this is requested by them. You must not start any new activity or project until you have received approval.

5.2 **You must inform the Data Subject before you use their information for the new purpose.** (e.g. update the relevant privacy notice). If consent is the current Lawful Ground relied on for the existing purpose, you must **obtain new consent** before you start any new activity or project.

## 6 USING THE LEAST AMOUNT OF PERSONAL DATA NEEDED TO ACHIEVE THE AIM (DATA MINIMISATION)

**You must only access and use the personal data you need to perform your role.** Accessing personal data that you are not authorised to access or that you have no reason to access may result in disciplinary action. If you have received or accessed information in error, you should let our Data Protection Lead know as soon as possible.

## 7 KEEPING PERSONAL DATA SAFE

7.1 **You must be able to recognise and report a suspected data breach.** If you believe there has been a data breach you must contact our Data Protection Lead immediately.

7.2 **You must abide by our processes and policies.** We provide training on how to use our IT systems and handle hard-copy information (e.g. clear desk policy, use of confidential waste bin). You must not try to override or circumvent technical measures we put in place to protect information (e.g. user permissions) and you must follow organisation measures we implement (e.g. attend staff training).

7.3 **Keep your logins and passwords confidential (do not share accounts).** Your account credentials, passwords and other information provided as part of our security procedures are confidential. It is your responsibility to keep your login information secure and you must notify our Data Protection Lead if you think your account has been accessed by someone else (or otherwise compromised).

## 8 SHARING PERSONAL DATA WITH OTHERS

8.1 **You must only share personal data internally which is required for the recipient's role (and you should follow IT sharing procedures).** It is important to remain diligent even when sharing information within the company. It is not always appropriate to share information with another person or team (e.g. disciplinary outcome shared with marketing team). If you are uncertain you should check with our Data Protection Lead before you share any information. You should follow IT best practice guidelines (e.g. password protect files, send links rather than attachments to documents) and maintain a clear desk policy.

8.2 **You must only share personal data externally where we have a contract (unless there is a legal exception).** It is mandatory to have a contract in place where organisations share information (which are called data processing agreements). These agreements set out which organisation is the Controller and which is the Processor.

8.3 **Where the recipient is outside the United Kingdom or the European Economic Area there are additional requirements.** You must check with our Data Protection Lead before you send any personal data to an organisation or person who is located (or whose servers are located) in a country outside the United Kingdom or European Economic Area.

8.4 **Where the disclosure is required by law, you need to disclose Personal Data.** In exceptional circumstances you might be contacted by an external organisation (e.g. police, solicitor) who requests personal data. You must refer these requests to our Data Protection Lead as soon as possible so that they can evaluate the request and decide whether to respond on behalf of us. You must not release any information unless you are instructed by our Data Protection Lead.

8.5 **You must be able to recognise when you have received a Data Subject access request (and other data right requests).** Individuals are granted specific rights under data protection law, one of which is the right to access information about them. If you receive a Data Subject right request, you must notify our Data Protection Lead as soon as possible. You can learn more about Data Subject rights and your responsibilities in the Data Protection Requests Policy.

## 9 DELETING (OR RETURNING) PERSONAL DATA THAT IS NO LONGER NECESSARY

9.1 **You must securely delete information at the end of its retention period.** We maintain a compliance document which lists how long we retain (keep) information, called the **Data Retention Policy**. When the period expires, you must delete or destroy the information and any copies of the information in line with the relevant procedure (e.g. confidential waste for hard copy information). We check all our information at least annually to ensure we continue to comply with our Data Retention Policy. You must always check our Data Retention Policy and, if you are unsure, our Data Protection Lead before you delete information.

9.2 **You must return (or delete) personal data that does not belong to us when instructed to do so.** Where we use, store or access personal data on behalf of another organisation (e.g. our business customers), we act as the Processor. We always have a contract with the other organisation where we process personal data. At the end of the contract, you must contact the other organisation to request their instruction as to whether you should delete or return their personal data.

9.3 **You must check before you fulfil a Data Subject request to erase (delete) their personal data.** Data protection law entitles individuals to ask organisations to delete their personal data. You receive this type of request, you must notify our Data Protection Lead as soon as possible. You can learn more about Data Subject rights and your responsibilities in the Data Protection Requests Policy.

## 10 THE COMPLIANCE RECORDS WE KEEP

10.1 **You must be aware of the different compliance records we keep.** We have up-to-date compliance records which help us to understand how the business uses personal data and ensure that we use it in a safe way and only for permitted purposes. The directors are responsible for ensuring compliance records are maintained (and reviewed at least annually) but you should be aware of the compliance records so you understand why you are required to provide certain information or take specific action. The records we keep include:

10.1.1 **Record of Processing Activities (ROPA):** We use this document to set out key information we use when we act as a Processor and Controller. It states the:

- purpose we are processing personal data (e.g. staff administration);
- Lawful Grounds we rely on (e.g. fulfil employment contract);
- categories of individuals (e.g. our workers, emergency contacts);
- types of types of personal data (e.g. payroll information, contact details);
- Where we act as a Processor, we also include the details of the organisation that is the Controller;

10.1.2 **Retention Schedule:** We use this document to identify when we should securely destroy information. It groups categories of information (e.g. HR files) and sets a clear expiry date (e.g. six years after an employee's final working day);

10.1.3 **Incident Report:** We use this document to record any suspected data breaches. It sets out what data was affected and what action we took (e.g. whether the incident was formally reported). We use it to help us improve the ways we keep information safe (e.g. update staff training, install additional

security features).

10.2 You must assist Data Protection Lead maintain our compliance records and act on their instructions (e.g. provide information, delete records) to ensure that our compliance documents can be properly maintained.

## 11 IF YOU HAVE ANY QUESTIONS ABOUT THIS POLICY

You should speak to our Data Protection Lead. They can be contacted at:

Email: info@cosecrecruitment.com

## 12 KEEPING THIS POLICY UP TO DATE

This policy was created on 9 October 2023 and will be reviewed and updated annually, or sooner if required by data protection laws.