exertis

Data Protection Policy

On the handling of Employee and Third Party data

Policy Owner: Legal & Compliance
Revision date: January 2023

a DCC business

Introduction

EXERTIS (UK) LTD (Exertis) is committed to doing business with integrity which includes taking good care of the personal information, of our employees, customers and other people, that we use as part of doing business.

The processing of personal information is integral to many of our operations. It ensures that we can meet the expectations of our customers and improve our service to them. Personal information is also essential in how we look after our employees. The people whose information we use trust us to safeguard that information.

If we fail to put in place the right controls to ensure that personal information is not abused, lost, passed to unauthorised parties or allowed to become out of date, then we lose the trust of those whose information we are looking after and we might also be breaking the law.

The General Data Protection Regulation ((EU)2016/679) (referred to as "EU GDPR") which was retained and forms part of the law of England and Wales, Scotland and Northern Ireland (referred to as "UK GDPR") and the Data Protection Act 2018 (together "Data Protection Legislation") provides rules in the UK which apply to the collection, use, disclosure, interception, monitoring and transfer abroad of information about individuals which includes employee and customer personal data. The Data Protection Legislation sets out the principles that Exertis must follow when processing personal data about individuals and also gives individuals certain rights in relation to personal data that is held about them.

Related legislation, the e-Privacy Regulation, sets out rules about use of personal data for marketing by email, SMS and telephone. Compliance with this policy will also address the requirements of the e-Privacy Regulation.

The aims of this policy are:

- To assist Exertis in meeting its obligations under the Data Protection Legislation;
- To regulate Exertis' use and collection of information relating to employees and others who work for Exertis (e.g. contractors or agents); and
- To ensure that employees and others working for Exertis are aware of both their rights in relation to the personal data that Exertis holds about them, and their responsibilities as regards personal data they may process about customers and other individuals as part of their job.

For ease of reference, this policy refers to "employees", but it applies equally to others working for Exertis, including consultants and contractors.

1. Data Protection Principles

The Data Protection Legislation is framed around clear data protection principles. Exertis and its employees must observe these data protection principles and be able to show that appropriate steps have been taken to ensure compliance with the principles. In summary these state that personal data must:

- Be obtained and processed fairly;
- Be used and disclosed for specified, explicit and legitimate purposes and not in any manner incompatible with those purposes;
- Be adequate, relevant and not excessive;
- Be accurate, complete and up-to-date;
- Not be kept for longer than is necessary for the purpose(s) for which it was obtained;
- Be processed in line with the rights given to individuals under the GDPR;
- Be kept safe and secure.

Importantly, Exertis must be able to demonstrate to the relevant authority that we have taken appropriate measures to ensure that we are complying with these principles.

All employees have an obligation to comply with these principles where appropriate.

What is Personal Data?

Personal data is data relating to a living individual who is or can be identified either from the data or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. The data protection principles apply to any sort of personal data which is either electronically processed (e.g. on a database) or which is held or intended to be in a structured filing system (e.g. a set of personnel files).

Certain personal data is classified as "sensitive personal data". This is personal data relating to a person's racial or ethnic origin, biometric or genetic data, political opinions, religious or philosophical beliefs, membership of a trade union, physical or mental health, sexual life or any criminal offence or related proceedings. For example, Exertis may, where necessary in connection with employment, collect and process sensitive personal data in respect of your health.

2. What We Have To Tell People When We Collect Their Information

When Exertis obtains information about an individual, we need to be transparent about who we are and how we will use the information. We always need to provide

- The identity of Exertis and contact details of the person responsible for data protection in Exertis;
- The purposes of the processing for which the information is being obtained as well as the legal basis for the processing (e.g. legitimate interests of Exertis);
- Who outside Exertis will receive the information (any such transfer to a third party needs to follow the rules in this Policy);
- Where applicable, the fact that Exertis intends to transfer the information to a company based in a country outside the UK and European Economic Area;
- Any additional information necessary to be fair and transparent in our use of the information. The period for which the information will be stored, or if that is not possible, how we determine that period;
- The existence of the right to request from Exertis access to and rectification or erasure of the information or restriction of our use of the information concerning or to object to our use of the information as well as the right to ask us to transfer the information to someone else;
- The existence of the right to withdraw consent at any time (if the use of information is based on consent);
- The right to lodge a complaint with the relevant regulating authority;
- Whether the provision of the information is a statutory (i.e. legal) or contractual requirement; and
- The existence of any automated decision-making (e.g. by a computer programme), and meaningful information about the process involved, the significance of, and the envisaged consequences of such use (e.g. where an individual is identified as being a priority delivery customer based on an analysis of data from other sources).

3. Employee Data

"Processing" includes the obtaining, recording, keeping and disclosing of data. Generally, processing of employee personal data is undertaken by Exertis for its legitimate interests, for example where the processing is necessary

for compliance with a legal obligation or where the processing is necessary for the performance of the employer / employee contract.

Nature of Employee Information

Exertis holds and processes certain information constituting personal data about you as part of its general employee records, which may include your address, contact details, payroll details, educational history, position, etc. Employee information is also held on HR and operational databases. In some cases, your manager might also hold employee information in his or her own files.

Sensitive personal data may include records of sickness absence, medical certificates and medical reports. The purpose of processing this type of information is generally to manage the application process, to administer benefit plans, to monitor and manage sickness absence and to comply with health and safety legislation. If sensitive personal data relating to you is being processed for reasons other than those set out above or otherwise permitted by law, your specific consent will be sought.

Purpose of Processing General Employee Information

Exertis needs to collect and use personal data about employees for a variety of personnel, administration, work and general business management purposes. These include administration of the payroll system, pension scheme, life insurance, the administration of employee benefits (such as leave entitlements), facilitating the management of work, carrying out appraisals, performance and salary reviews, operating and checking compliance with Exertis' employment rules and compliance policies, operating Exertis' IT and communications systems, checking for unauthorised use of those systems, protection of its legitimate business interests and to comply with record keeping and other legal obligations. Exertis considers this processing to be in its legitimate interest.

Keeping Employee Information

Exertis will take steps to ensure that the employee information it holds is accurate and up-to-date. For example, you are asked to inform Exertis of any changes which we need to make to update your employee information (such as a change of address). From time to time you will be asked to supply updated personal information as part of any periodic review of personal data held to ensure that Exertis meets its data protection obligations. Exertis will also take steps to ensure that it does not keep any information about employees for longer than is necessary.

Transfer of Employee Information

Exertis may make some information about you available to Exertis' advisers and/or data processors such as lawyers, accountants, payroll administrators, benefits providers (for example, pension scheme providers), to those providing products or services to Exertis (such as IT and other outsourcing providers) and to government and/or regulatory authorities. These recipients may be located outside the UK and European Economic Area. In such case, Exertis will ensure that the recipients of the information, both within and outside Exertis, comply with the contents of this policy and EU GDPR. Information about an employee may also be transferred to another company within the Group solely for purposes connected with career development or the management of the business.

If you are involved in transferring any data for processing on behalf of Exertis to a third party you must ensure that a Data Processing Agreement is signed by the third party.

Your Rights under the Data Protection Rules

The Data Protection Legislation gives you (and anyone else about whom personal data is held) specific rights in relation to the information that is held about you. Some of these rights are summarised below.

Under the Data Protection Legislation you have the right to:

- Know that information is being processed;

- Access information that is being processed;
- Rectification of information being processed;
- Erasure of information held on you (commonly known as the right to be forgotten);
- Restrict processing;
- Be notified about what information has been rectified, erased and restricted;
- Portability (that is, to request your data be handed over to someone else);
- Object to the processing of your information

It is important to note that this is not an absolute right to review all the information that is held about you, as there are various exceptions to this right contained in the Data Protection Legislation. These include:

(a) where personal data is kept for the purpose of preventing, detecting or investigating offences and related matters; and

(b) where the data is given by another person in confidence.

4. Your Responsibilities under the Data Protection Legislation

As well as having rights under the Data Protection Legislation, all employees, when processing personal data, must comply with the data protection rules set out in this policy. Failure to comply with the rules and requirements in relation to data protection may result in disciplinary action being taken against you. In particular please note the following:

Your Personal Information

In order to assist Exertis in ensuring that your personal information is kept up to date, you should inform the Exertis HR team of any changes in the following information:

- Address and other contact details;
- Emergency contact name;
- Bank account details; and
- Marital status

Personal Information Relating to Others

- If, as part of your job, you hold any personal information about other employees of Exertis or about anyone else (such as candidates in a recruitment process or customer personal information) then you also need to take steps to ensure that you are following the guidelines set out below. Please note that the following guidelines apply equally to documents containing personal information which are kept in files, as well as information which is kept electronically.
- You should not keep personal information about people which you no longer need or which is out of date or inaccurate. You should therefore review any personal information that you hold from time to time, bearing these principles in mind.
- All personal information must be kept securely and must remain confidential. You should be careful not to inadvertently disclose documents by sending data via email, reading sensitive documents in a public place or using laptops, smart phones etc. on public transport or in a public place.

- Sensitive data should be treated even more carefully. For example, you should keep sensitive data locked in a filing cabinet with restricted access and stored only on encrypted devices.
- If you receive a request from someone to give them any personal data about an employee (or other individual) you should refer them to the HR team. Exertis needs to verify the identity of the person making such a request and has to balance various considerations when deciding whether and how to respond to such request, including compliance with the
  Data Protection Legislation .
- Accessing, disclosing or otherwise using employee records or other personal data without authority will be treated as a serious disciplinary offence and may result in disciplinary action being taken in accordance with Exertis disciplinary procedure up to and including dismissal. If you breach this Policy as an individual then the relevant data protection regulator may take action directly against you.
- If you are sending data to a third party to do work for the company then remember to put in place a Data Processing Agreement unless data protection is covered in an existing master contract with Exertis.
- You must not send to Exertis suppliers personal data, including data contained in reports, containing personal information of customers or their customers in turn (e.g. drop ship end consumer data, second-tier sales out data or Exertis sales out data relating to individuals) unless our customer has (and/or its customers have) consented to the information being shared and there is an appropriate Data Processing Agreement in place with the supplier. If any supplier recipient is located outside the UK and European Economic Area, you must not send any customer personal data without first securing written approval from and putting in place all additional safeguards required by the person responsible for data protection in Exertis. This may require completion of a data protection impact assessment (see further **section 8** below).

If you are unsure about the application of these guidelines to the information you hold as part of your job, you should ask for advice from your manager. Training will be available to help you understand what you have to do.

Breach of this Policy will be a disciplinary matter and may result in sanctions being put in place against you under our disciplinary policy, up to and including dismissal.

5. Monitoring and Interception

You are entitled to know about any monitoring of electronic and telephone communications systems or CCTV surveillance that Exertis may undertake although this may take the form of notification to you via Exertis' Employee Handbook or contract of employment. CCTV monitoring will be indicated by signage although from time to time Exertis may have to undertake covert monitoring for purposes of security or otherwise to protect its legitimate business interests. Information about monitoring of electronic communications systems can be found in Exertis' CCTV Policy. All covert monitoring must be authorised by the director responsible for data protection following completion of a Monitoring Impact Assessment.

For some vehicles, Exertis might use telematic or vehicle tracking systems for safety, security and business efficiency purposes. Please see Exertis' Employee Handbook for more details.

6. Third Party Data (such as customer, suppliers, contractors etc.)

Our Commitment To Protecting the Personal Information Of Customers and Other Third Parties

Privacy of customer, supplier and contractor data is important to Exertis. To better protect customer privacy we provide a notice on our website to explain our information practices and the choices a customer can make about the way his or her information is collected and used. To make this notice easy to find, we make it available on our homepage www.exertis.co.uk.

The Way Exertis Uses Customer Information

Exertis uses the information a customer provides when placing an order only to complete that order, maintain high levels of customer service and to contact them about buying more of those products for a limited time afterwards. We do not share this information with outside parties except to the extent necessary to complete that order. On occasions it may be necessary for us to communicate with the customer for administrative or operational reasons relating to the services provided.

We use return email addresses to answer the email we receive. Such addresses are not used for any other purpose, apart from and are not shared with outside parties.

When obtaining customer contact details, Exertis will either rely on its legitimate interest to market its products to customers or will seek the customer's permission about use of the customer's data and contact preferences. Where there is a legitimate interest or the customer has consented, contact details may be used to supply information to the customer by telephone, SMS, email or post, about Exertis and to send occasional promotional material, such as information about special offers which we think the customer might find valuable. We must always make clear that the customer may opt out from receiving future information at any time; we can only contact the customer by post if the customer has specifically opted in to receive communications from us or we have another legitimate business purpose (such as marketing or account management) for contacting them.

Marketing by email or telephone is governed by slightly different rules. In general, we are allowed to market to customers by email or telephone if they have provided their contact details to us as part of a transaction in which they bought goods from us – for a limited period (see our retention policy) we can use the details they provided to market to them more of the products which they originally purchased.

Our Commitment To Data Security

To prevent unauthorised access, maintain data accuracy, and ensure the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect. Access to the information which is provided by customers will be limited to authorised employees as required for the purposes identified above as well as IT security and maintenance.

Any personal information provided by a customer may be used to verify the customer's identity and assist Exertis in preventing or detecting fraud. As part of these checks customer information may be disclosed to credit reference agencies, who may keep a record of that information. This is not a credit check and the customer's credit rating will be unaffected.

Customer / Third Party Access To or Correction of Information Held About that Customer

A customer is able to withdraw his or her consent to processing or request access to all of his or her personal information that we collect online and maintain by completing the online request form accessible on the GDPR Portal section of the main Exertis website: www.exertis.co.uk.

To protect privacy and security, we must take reasonable steps to verify the customer's identity before granting access or making corrections.

The customer will need to confirm in writing (including by email) their full name, full address, date of birth and a description of the information required.

The Data Protection Legislation allows Exertis one month to provide the requested personal information. This starts from the date we receive the request containing enough information for us to identify the customer and locate the information requested and proof of identity (e.g. photocopy of driving licence). However, Exertis will try to provide this information as soon as possible within this time-scale.

A customer can correct factual errors in his or her personal information that we hold by sending us a request that credibly shows that there is an error in our records.

Data protection rights exist in voice and video recordings. We must treat video and voice recordings in the same way we treat other personal data:

Voice Recordings

In the event of a disputed fact arising from a telephone conversation which has been recorded, the recording of the relevant part of the conversation may be disclosed to the customer, provided a release form has been completed and approved by the director responsible for data protection, and a copy must be retained on file.

Video Recordings

Any request for access to video recordings should be dealt with in accordance with the Exertis CCTV policy.

Processing of Information by Service Providers on Our Behalf

Exertis will sometimes need to use a third party to provide services on its behalf which will involve the use of customer or employee information, for example a mailing house for marketing purposes, outsourced IT solutions or a payroll services provider for the HR team.

If you are involved in transferring any data for processing on behalf of Exertis to a third party you must ensure that a Data Processing Agreement is signed by the third party and that an appropriate IT security risk assessment is performed by the IT Security Manager.

Requests For Information By Police etc.:

Requests from the police and government departments are not data subject access requests but classed as requests for disclosure by a third party. The Data Protection Legislation expressly provides that such requests may be exempt from the data protection principle regarding restriction of access to personal data if the conditions set out in the relevant exemptions apply, namely that there is a statutory right for them to have access to that information.

Although these are not subject access requests Exertis must maintain a good audit trail, good tracking system and ensure that all disclosures are properly recorded with reasons given for the disclosure.

All requests that have been received by Exertis should be referred to the director responsible for data protection who will log the request and handle the response process.

Any such request from the police, tax authorities or other government department should be referred to the director responsible for data protection. Please note that private organisations are not authorised to investigate criminal activity so the exemption may not apply.

The director responsible for data protection will:

Maintain a log of all requests;

- Ensure these written requests are signed off by someone in authority in the requesting organisation in a formal request;
- Maintain a copy of information sent in response;
- If redactions (i.e. black outs) are applied, reasons for the redaction are to be maintained;
- Ensure that sent documents are signed off by the relevant manager; and
- Ensure appropriately secure mode of despatch e.g. recorded delivery, encryption.

For every request for personal information received through a formal request, the director responsible for data protection will ask the following questions:

- Am I sure the person is who they say they are (only formal written requests are to be processed)?
- Is the person asking for this information doing so under a statutory power or under a court order – obtain written confirmation?
- If I do not release the personal information, will this significantly harm any attempt by the requesting authority to prevent crime or catch a suspect?
- If I do decide to release personal information, what is the minimum I should release for them to do their job?
- What else (if anything) do I need to know to be sure that the exemption applies?

7. Privacy By Design: Recording Decisions Which Affect Data Protection

The Data Protection Legislation introduces the concept of a data protection impact assessment (a "DPIA"), which is a requirement when the business processes personal data which is "likely to result in a high risk to the rights and freedoms" of the subject of the data.

We will use DPIAs as a compliance tool to describe, assess and mitigate the risks to an individual's rights and freedoms from the processing of personal data and also to demonstrate that measures we will take to ensure compliance.

The minimal requirements for a DPIA are that the assessment shall contain at least:

- A systematic description of the envisaged processing operations and the purposes of the processing
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- An assessment of the risks to the rights and freedoms of data subjects; and
- The measures envisaged to address the risks.

We will always carry out a DPIA prior to introducing any new data processing or where changes to an existing process will have an impact on personal data. The ultimate accountability for ensuring a DPIA is in place lies with the data controller. Failure to comply with DPIA requirements under the Data Protection Legislation can result in very substantial fines.

A single DPIA may be used for a single processing operation or to address a set of similar processing operations that present similar high risks, as long as sufficient consideration is given to the nature, scope, context and purpose of the processing. Situations that may particularly indicate a high risk which will require a DPIA include where we undertake the following:

- Evaluation or scoring, including profiling or predicting;
- Automated decision making with legal or similar significant effect;
- Monitoring;
- Processing of sensitive data;
- Data processed on a large scale;
- Datasets that have been matched or combined;
- Data concerning vulnerable data subjects;
- Innovative use or applying technological or organisational solutions;
- Data transfer across borders outside the European Economic Area; and
- Where the processing itself prevents data subjects from exercising a right or using a service or contract.

The DPIA will be a record of our decision-making process where we are taking any steps that have an impact on personal data in our business. A record of all DPIAs will be retained centrally by the director responsible for data protection.

8. Any Questions About Data Protection or this Policy

If you have any questions about this policy or if you receive any questions from customers or third parties about data protection, please complete the online contact form on the GDPR Portal on the main Exertis website www.exertis.co.uk or email dataprotection@exertis.co.uk. The director responsible for data protection is Michael Sudlow.

9. Related Policies

There are a number of Exertis policies related to this policy which you are advised to read in conjunction with this policy:

CCTV Policy

Document Retention Policy

IT Information Security Policy

Employee Handbook

Social Media Policy