# EXERTIS IRELAND LIMITED DATA PROTECTION POLICY ON THE HANDLING OF EMPLOYEE AND THIRD PARTY DATA

## 1. Introduction

**EXERTIS Ireland Limited and related companies** (**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controls to ensure that personal information is not abused, lost, passed to unauthorised parties or allowed to become out of date, then we lose the trust of those whose information we are looking after and we might also be breaking the law.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 2016 (referred to as the "GDPR") provides rules which apply to the collection, use, disclosure, interception, monitoring and transfer abroad of information about individuals which includes employee and customer personal data. The GDPR 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 GDPR;
- 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.

## 2. Data Protection Principles

The GDPR 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.

## 3. 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 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).

## 4. 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 [director] using the Impact Assessment form at Schedule 1.

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.

## 5. 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 and in our marketing publications 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 and at every point where we may request personal information from a customer or third party.

### 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, or similar, 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, and are not shared with outside parties without explicit consent.

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 - you must always check with the relevant team before using any personal data for email or telephone marketing respectively. 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 writing to Director Responsible for Data Protection, Exertis Ireland, M50 Business Park, Ballymount Ave, Ballymount, Dublin 12.

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 ffull name, full address, date of birth and a description of the information required

The GDPR 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 timescale.

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 the release form in Schedule 2 has been completed, a copy to 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 director responsible for data protection and by the third party (see schedule 3) and that an appropriate IT security risk assessment is performed by the local security officer(see schedule TBD).

**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 GDPR 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?

## 6. Privacy By Design: Recording Decisions Which Affect Data Protection

The GDPR 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. More details are set out in our DPIA Policy.

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 GDPR 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;
- systematic 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 Union; 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 director responsible for data protection.

## 7. **Any Questions About Data Protection or this Policy**

All questions from customers or third parties about Exertis data protection policy should be referred to director responsible for data protection.

## 9. **Related Policies**

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

CCTV Policy

Document Retention Policy

IT Security Policy

Third Party IT Security Risk Assessment Template

Privacy Policy

Employee Handbook

Social Media Policy

## **Schedules**

Schedule 1: Monitoring Impact Form

Schedule 2: Voice Recording Release Form

Schedule 3: Data Processing Agreement

Schedule 4: Data Protection Impact Assessment Template

**Schedule 1**

**Exertis: EMAIL / TELEPHONE ACCOUNT ACCESS: MONITORING IMPACT ASSESSMENT**

**A. The Law:** Data Protection legislation controls the monitoring by an employer of electronic communications including emails, faxes and telephone records / lines. **Any monitoring can only be undertaken with the approval of the company's** director responsible for data protection **or IT Director/Head of IT and must be in compliance with our Data Protection and IT Security Policies.**

**B. Remember:**
1. Monitoring is usually intrusive.
2. Employees legitimately expect to keep their personal lives private.
3. Employees are entitled to some privacy in the work environment.

Before undertaking any monitoring or interception of communications read the following:

- Consider whether alternative approaches or different methods of monitoring would deliver the benefits you want while being more acceptable to employees. Can you target the monitoring. For example: emails to specific suppliers; telephone calls to recognised numbers or emails to specifically identified individuals?
- Ensure employees are aware that they are being monitored and why. The IT security policy and contracts of employment both state that we may undertake monitoring for business compliance purposes. If a specific project requires monitoring than an e-mail could be sent about the monitoring. We should be open about any monitoring, so that employees know what to expect.
- Where monitoring is used to enforce rules and standards, make sure that these rules and standards have been clearly communicated.
- Only use information obtained through monitoring for the purpose for which you carried out the monitoring, unless the monitoring leads to the discovery of an activity that no employer could reasonably be expected to ignore, for example breaches of health and safety rules that put other workers at risk or other forms of gross misconduct.
- Keep secure the information that you gather through monitoring. This might mean only allowing one or two people to have access to it. Don't keep the information for longer than necessary or keep more information than you really need. This might mean deleting it once disciplinary action against an employee is over.
- If you need access to an employee's email account (for example if the employee has left the business or is absent) then only open emails relevant to your investigation or business needs. Do not open or read any clearly personal emails. Where the employee has left the business, personal emails should be deleted.
- The covert monitoring of communications can rarely be justified. Do not carry it out unless it has been properly authorised in your business (byIT Director/Head of IT, Human Resources Director, and the director responsible for data protection). You should be satisfied that there are grounds for suspecting criminal activity, or equivalent gross misconduct, and that telling people about the monitoring would make it difficult to prevent or detect such wrongdoing.

**C. Answer the following questions:**

| CONSIDERATION | RESPONSE |
|---|---|
| What form of monitoring is intended? | |
| Name of employee or group of employees affected. | |
| Can you confirm that the monitoring is in the legitimate interest of the business? | Yes / No * |
| Who will undertake the monitoring? | Director or above……(name) |
| What is the purpose of the monitoring? | Business information / disciplinary action / service standards / breach of compliance guidelines * |
| Is there a risk that personal data will be viewed? | Yes / No * |
| The nature of information monitored will be? | Personal / business * |
| Has any less intrusive alternative been tried? If not, why not? | Yes / No * |

(*delete as appropriate)

**D. Compulsory Rules for Monitoring:**

1. **only those authorised by this Impact Assessment may conduct the monitoring;**
2. **data must be retained confidentially and destroyed as soon as they have served their purpose; and**
3. **data may only be used for the purpose authorised by this Impact Assessment.**

**E. AUTHORISATION:**

Director [responsible for Data Protection]:……signed & print name

HR Director/Senior HR Managerr:……..signed & print name

IT Director / Head of IT……signed & print name

Date:……

NB Once approved this document is to be kept with the relevant personnel file.

**Schedule 2**

**Voice Recording Release Form**

**RELEASE OF VOICE RECORDING - POLICE AND CUSTOMER**

| | |
|---|---|
| Name of person making request: | |
| Organisation: | |
| Address: | |
| Telephone Number: | |

**DETAILS OF RECORDING TO BE RELEASED**

| | |
|---|---|
| Date: | |
| Reason (e.g. to evidence details of agreed order involving customer to whom recording will be released): | |

| | | | |
|---|---|---|---|
| Signed<br>(Director with responsibility for Data Protection): | | Dated: | |
| Request Granted: | | Request Denied (Reason): | |

**Schedule 3**

**Exertis Template Data Processing Agreement**