

DATA PROTECTION POLICY

ISO 27001:2022 Annex A Clause 5.34

Oakray is committed to fulfilling their responsibilities under the requirements of the General Data Protection Regulation (GDPR) and all other data protection legislation currently in force. We recognise the rights of individuals to respect for the privacy of their personal details and will only collect and process information when there is a legitimate need to do so.

INTRODUCTION

This policy describes how Oakray will collect, process and use sensitive personal data and the rights that staff and other data subjects have to access data held about them.

All employees who collect, process or have access to sensitive personal data are required to comply with this policy. Any failure to follow the policy may result in action being taken under Oakray's disciplinary procedure.

More detailed information for managers on the collection and processing of personal data is given in the guidance note 'Data Protection at Oakray – What you Need to Know', which is available from the HR Department.

DATA PROTECTION GDPR

The Company is fully committed to comply with the requirements of the General Data Protection Regulation (GDPR). The Regulation applies to anyone processing personal data. It sets out principles which should be followed and it also gives rights to those whose data is being processed.

To this end, the Company endorses fully and adheres to the Data Protection Principles listed below. When processing data we will ensure that is:

- Processed lawfully, fairly and in a transparent way ('lawfulness, fairness and transparency'); and
- Processed no further than the legitimate purposes for which that data was collected ('purpose limitation')
- Limited to what is necessary in relation to the purpose ('data minimisation'); and
- Accurate and kept up to date ('accuracy'); and
- Kept in a form which permits identification of the data subject for no longer than is necessary ('storage limitation'); and
- Processed in a manner that ensures security of that personal data ('integrity and confidentiality'); and
- Processed by a controller who can demonstrate compliance with the principles ('accountability')

These rights must be observed at all times when processing or using personal information. Therefore, through appropriate management and strict application of criteria and controls, the Company will:

- Observe fully the conditions regarding having a lawful basis to process personal information
- Meet its legal obligations to specify the purposes for which information is used

- Collect and process appropriate information only to the extent that it is necessary to fulfil operational needs or to comply with any legal requirements
- Ensure the information held is accurate and up to date
- Ensure that the information is held for no longer than is necessary
- Ensure that the rights of people about whom information is held can be fully exercised under the GDPR (i.e. the right to be informed that processing is being undertaken, to access personal information on request; to prevent processing in certain circumstances, and to correct, rectify, block or erase information that is regarded as wrong information)
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred outside the EU, to other countries or international organisations without an adequate level of protection

Employee's personal information

Throughout employment and for as long as is necessary after the termination of employment, the Company will need to process data about you. The kind of data that the Company will process includes:

- any references obtained during recruitment
- details of terms of employment
- payroll details
- tax and national insurance information
- details of job duties
- details of health and sickness absence records
- details of holiday records
- information about performance
- details of any disciplinary investigations and proceedings
- training records
- contact names and addresses
- correspondence with the Company and other information that you have given the Company

The Company believes that those records used are consistent with the employment relationship between the Company and yourself and with the data protection principles. The data the Company holds will be for management and administrative use only but the Company may, from time to time, need to disclose some data it holds about you to relevant third parties (e.g. where legally obliged to do so by HM Revenue & Customs or where requested to do so by yourself for the purpose of giving a reference or in relation to maintenance support and/or the hosting of data in relation to the provision of insurance).

In some cases, the Company may hold sensitive data, which is defined by the legislation as special categories of personal data, about you. For example, this could be information about health, racial or ethnic origin, criminal convictions, trade union membership, or religious beliefs. This information may be processed not only to meet the Company's legal responsibilities but, for example, for purposes of personnel management and administration, suitability for employment, and to comply with equal opportunity legislation. Since this information is considered sensitive, the processing of which may cause concern or distress, you will be asked to give express consent for this information to be processed, unless the Company has a specific legal requirement to process such data.

Access to Data

You may, within a period of one month of a written request, inspect and/or have a copy, subject to the requirements of the legislation, of information in your own personnel file and/or other specified personal data and, if necessary, require corrections should such records be faulty. If you wish to do so you must make a written request to your line Manager. The Company is entitled to change the above provisions at any time at its discretion.

Data security

You are responsible for ensuring that any personal data that you hold and/or process as part of your job role is stored securely.

You must ensure that personal information is not disclosed either orally or in writing, or via web pages, or by any other means, accidentally or otherwise, to any unauthorised third party.

You should note that unauthorised disclosure may result in action under the disciplinary procedure, which may include dismissal for gross misconduct. Personal information should be kept in a locked filing cabinet, drawer, or safe. Electronic data should be coded, encrypted, or password protected both on a local hard drive and on a network drive that is regularly backed up. If a copy is kept on removable storage media, that media must itself be kept in a locked filing cabinet, drawer, or safe.

When travelling with a device containing personal data, you must ensure both the device and data is password protected. The device should be kept secure and where possible it should be locked away out of sight i.e. in the boot of a car. You should avoid travelling with hard copies of personal data where there is secure electronic storage available. When it is essential to travel with hard copies of personal data this should be kept securely in a bag and where possible locked away out of sight i.e. in the boot of a car.

USE OF CCTV

CCTV cameras are installed in a number of locations in Oakray and the surrounding precincts, and images are monitored and recorded for the purposes of crime prevention and for the safety and security of visitors and members of the public.

The management of CCTV surveillance is carried out in accordance with the ICO CCTV Code of Practice 2008. The scheme is controlled by the Facilities Manager.

Only employees who have received relevant training and hold an SIA licence are permitted to have access to the CCTV system. Staff who misuse CCTV images in any way will be subject to action under Oakray's disciplinary procedures and may also face criminal prosecution.

CCTV cameras are not installed for the primary purpose of monitoring employees. If, however, an employee is facing allegations of misconduct then CCTV images may be used to provide evidence to a disciplinary investigation or a disciplinary hearing.

DIRECT MARKETING AND FUNDRAISING

In carrying out any direct marketing and fundraising activities Oakray must comply with both the provisions of the General Data Protection Regulation and the Privacy and Electronic Communications (EC Directive) Regulations 2003.

In order to comply with the Regulations Oakray will not hold or process any personal information on individuals for any purpose without their prior consent. In obtaining that consent we must tell individuals:

- What their information will be used for
- How they will be contacted – e.g. post, phone or email
- Our policy on passing information to other organisations

We must also obtain consent before any marketing or fundraising information is sent to the individuals on whom we hold personal details. This only needs to be done once, and can be done at the same time as requesting consent to hold their data. It is, however, good practice to give individuals the chance to opt out of receiving further marketing communications each time they are contacted. If an individual request not to receive any further marketing communications this request must be actioned immediately.

Any employee who does not comply with this policy may be subject to action under Oakray's Disciplinary Policy.

RIGHT TO ACCESS INFORMATION UNDER GDPR

Under the GDPR, the right of access grants data subjects the right to obtain confirmation from the controller as to whether or not their personal data is being processed.

The GDPR clarifies that the reason for allowing individuals to access their personal data is so that they are aware of – and can verify the lawfulness of – the processing.

Upon request, data subjects are entitled to access their personal data, and to receive details about the following:

- The purposes of the processing
- The categories of data that are being processed
- The recipients of the data (and if they are located in third countries, any safeguards, if applicable)
- The envisaged storage period (where it is possible to estimate this) or the criteria that will determine that period
- The data subject's rights
- The existence of automated decision-making (including profiling), as well as the logic involved, the significance and the envisaged consequences of such processing for the data subject
- Any available information regarding the source of the data (in cases where data is not collected directly from the data subject)

The information must be provided to the data subject without delay, and within one month of receipt of the request at the latest. In the event that a request is complex, the compliance period can be extended by two months (in which case the controller must inform the data subject of the reason for the delay within one month of receiving the request).

Moreover, the information must be provided using reasonable means – for example, if the request was made electronically, the information should be provided in a commonly used electronic format.




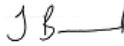

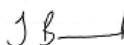
The information should also be provided free of charge, although a reasonable fee can be charged if the request is unfounded or excessive.

Where requests are clearly unfounded or excessive (e.g. if they are repetitive), the controller can choose to refuse the request. In that event, the controller must inform the data subject of the reason(s) for refusal and must inform them of their right to complain to the supervisory authority.

DATA CONTROLLER

Oakray has an appointed Data Protection Officer who acts as the Data Controller under the General Data Protection Regulation. All enquiries regarding the Data Protection Policy should be sent to the DPO (dpo@oakrays.co.uk).

Document History*(For previous version changes, please look to the document control spreadsheet)*

Version Number	Date	Created by	Signature	Approved	Signature	Description	Review date
3	30/06/21	Sandra Greenaway		Wayne Dejager		Annual Review	30/06/22
4	08/06/22	Sandra Greenaway		James Barnard		Annual Review, change of Director	08/06/23
5	20/06/23	Nick Quail		James Barnard		Annual Review	20/06/24