# Employee privacy notice

## Introduction

Ecclesiastical Insurance Office plc (the Company) is committed to protecting the personal data of its employees. This Notice sets out important information about how the Company and its associated companies collect and use your personal data during the course of your employment and after your employment has ended.

You should read this Notice carefully and raise any questions you may have with the HR team or Data Protection Officer.

## Scope

This Notice applies to employees located in the Republic of Ireland. In connection with your employment, the relevant data controller is Ecclesiastical Insurance Office plc (company number 24869) whose registered office is Benefact House, 2000 Pioneer Avenue, Gloucester Business Park, Brockworth, Gloucester, GL3 4AW.

## What personal data do we collect?

Personal data means information which identifies you and relates to you as an individual. As your employer, the Company will collect, use and store your personal data for a wide variety of reasons in connection with the employment relationship. We have set out below the main categories of employee personal data which we process on a day to day basis:

- personal contact information (including your name, home address, personal telephone number(s) and personal e-mail address)
- business contact information (including e-mail address and telephone number)
- job title and corporate grade
- date of birth
- PPS number, passport details and / or driving licence number
- gender
- marital status
- emergency contact information including dependant details
- photograph
- documents evidencing your right to work (including information about your immigration status where relevant)
- bank account details
- documents gathered during the recruitment process (including cv, application form, references, professional memberships and qualifications, background vetting information)
- general employment records including details of training, disciplinary and grievance matters, benefits, holiday and other absences, along with a copy of your employment contract, performance records (including appraisals) and salary history
- information gathered through the Company's monitoring of its IT systems, building access records and CCTV recording
- personal data which you otherwise voluntarily provide, for example when using your company e-mail account
- Payroll data including tax code

The majority of the personal data provided by you is mandatory in order for us to administer the employment relationship and/or comply with statutory requirements relating to immigration or taxation. Failure to provide mandatory personal data may affect our ability to accomplish the purposes stated in this Notice and potentially affect your ongoing employment.

The list set out above is not exhaustive, and there may be other personal data which the Company collects, stores and uses in the context of the employment relationship. We will update this Notice from time to time to reflect any notable changes in the categories of personal data which it processes.

The majority of the personal data which we process will be collected directly from you. In limited circumstances your personal data may be provided by third parties, such as former employers, official bodies (such as regulators) and/or medical professionals.

## How do we use your personal data?

The Company uses your personal data for a variety of purposes in order to perform its obligations under your employment contract, to comply with legal obligations or otherwise in pursuit of its legitimate business interests. We have set out below the main purposes for which employee personal data is processed:

- the payment of salary and the administration of benefits under the employment contract
- the day to day management of tasks and responsibilities
- to manage performance, including the conduct of annual appraisals
- to consider eligibility for promotion or for alternative roles within the Company
- to comply with legal requirements, such as reporting to the local tax authority
- to address disciplinary and grievance issues with individual employees
- to protect the Company's confidential and proprietary information, and intellectual property
- to monitor the proper use of the Company's IT systems
- to prevent fraud against the Company and its clients
- if a business transfer or change of ownership occurs

Again, this list is not exhaustive and the Company may undertake additional processing of personal data in line with the purposes set out above. The Company will update this Notice from time to time to reflect any notable changes in the purposes for which it processes your personal data.

## What special categories of personal data to we process?

Certain categories of data are considered "special categories of personal data" and are subject to additional safeguards. The Company limits the special categories of personal data which it processes as follows:

- **Health Information**

  The Company will process information about an employee's physical or mental health in compliance with its obligations in connection with employment, in particular (i) to administer Company sick pay; (ii) to facilitate the provision of benefits, such as private medical insurance; (iii) to comply with obligations owed to disabled employees; (iv) to comply with health and safety obligations; and (v) to maintain a sickness absence record.

We will always treat information about health as confidential and it will only be shared internally where there is a specific and legitimate purpose to do so. We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure.

Health information will typically be retained during the course of an individual's employment. Following the termination of an individual's employment, we will typically retain health information for 6 years subject to any exceptional circumstances and/or to comply with particular laws or regulations.

- **Criminal Record Information**

  Given the nature of our business and our responsibilities to our clients, we ask employees to disclose their criminal record history via a Criminal Record Declaration as part of our background vetting process and in compliance with our obligations in connection with employment.

  We will always treat criminal record history as confidential and it will only be shared internally where there is a specific and legitimate purpose to do so. We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure.

  Criminal record declarations will typically be retained for a maximum of 6 months, although the outcome of any check will remain on the employee's record.

- **Equal Opportunities Monitoring**

  The Company is committed to providing equal opportunities for employment and progression to all of its employees and from time to time it will process information relating to ethnic origin, race, nationality, sexual orientation and disability, alongside information relating to gender and age, for the purposes of equal opportunities monitoring.

  We have implemented appropriate physical, technical, and organisational security measures designed to secure your personal data against accidental loss and unauthorised access, use, alteration, or disclosure. In addition, this monitoring will always take place in accordance with appropriate safeguards as required under applicable law, including:

  - the provision of information relating to ethnic origin, race, nationality, sexual orientation and disability for the purposes of monitoring will be voluntary

  - wherever possible, the monitoring will be conducted on the basis of using anonymised data so individual employees cannot be identified

## When do we share employee personal data?

The Company will share employee personal data with other parties only in limited circumstances and where this is necessary for the performance of the employment contract or to comply with a legal obligation, or otherwise in pursuit of its legitimate business interests as follows:

- payroll providers
- benefits providers
- background vetting specialists
- occupational health providers

- Revenue and/or any other applicable government body
- accountants, lawyers and other professional advisers
- the Financial Conduct Authority and/or the Prudential Regulatory Authority and/or the Central Bank of Ireland and/or any other applicable regulatory body
- the Information Commissioner's Office

Wherever possible, the employee personal data is shared under the terms of a written agreement between the Company and the third party which includes appropriate security measures to protect the personal data in line with this Notice and our obligations. The third parties are permitted to use the personal data only for the purposes which we have identified, and not for their own purposes, and they are not permitted to further share the data without our express permission.

## For how long will my personal data be retained?

The Company's policy is to retain personal data only for as long as needed to fulfil the purpose(s) for which it was collected, or otherwise as required under applicable laws and regulations. Under some circumstances we may anonymise your personal data so that it can no longer be associated with you. We reserve the right to retain and use such anonymous data for any legitimate business purpose without further notice to you.

Following the termination of an individual's employment, the Company will typically retain data for the periods set out below subject to any exceptional circumstances and/or to comply with particular laws or regulations:

- general personnel file documents: 2 years
- contractual documentation 7 years
- regulatory reference information 6 years
- records relating to tax and social security contributions: 7 years
- information relating to pensions or other ongoing benefits 7 years
- personal data held in archived e-mails or other electronic files: indefinitely

For more information please refer to our Group Retention Policy which can be accessed on the Company's intranet.

## What is our approach to sending your personal information overseas?

There may be some instances where your personal information is transferred to countries outside of the European Economic Area ("**EEA**") such as when we transfer information to our third party suppliers who are based outside the EEA or when third parties who act on our behalf transfer your personal information to countries outside the EEA.

Where such a transfer takes place, we will take the appropriate safeguarding measures to ensure that your personal information is adequately protected. We will do so in a number of ways including:

- entering into data transfer contracts and using specific contractual provisions that have been approved by European data protection authorities otherwise known as the "standard contractual clauses";
- transferring personal data only to companies in the United States who are certified under the "Privacy Shield" framework. The Privacy Shield is a scheme whereby companies certify that they

provide an adequate level of data protection. You can find out more about the Privacy Shield at www.privacyshield.gov;

- we will only transfer personal data to companies in non-EEA countries who have been deemed by European data protection authorities to have adequate levels of data protection for the protection of personal information. You can find out more about this at ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en; or
- transferring personal data to multinational companies who have put in place Binding Corporate Rules (BCRs) which have been authorised by a data protection authority. You can find out more about this atico.org.uk/for-organisations/binding-corporate-rules.

We are also entitled under European data protection laws to transfer your personal information to countries outside the EEA in the following circumstances:

- it is necessary for the performance of the contract we have with you; or
- it is necessary to protect your vital interests i.e. it is a life or death situation.

Depending on our relationship and your particular circumstances, we might transfer personal information anywhere in the world. A summary of our regular data transfers outside the EEA is set out below:

| **Country of transfer** | **Reason for the transfer** | **Method we use to protect your information** |
|---|---|---|
| Singapore | The provider of the Employee Online Benefits System (Thomsons Online Benefits Limited) uses an affiliate based in Singapore to provide its administration and support services. | We have entered into standard contractual clauses with the provider and their affiliate. The provider is a subsidiary of Marsh & McLennan Companies, Inc (MMC). MMC have put in place BCRs which have been authorised by the Information Commissioner, a copy of which can be found at www.uk.mercer.com/data-protection.html. |
| USA | If you opt in for the employee benefit of Pension Vouchers, the provider of this benefit (VouchedFor Limited) uses third party suppliers for its customer service programme and to store and transfer data between systems. | The USA has been deemed to offer an adequate level of protection for personal data transfers covered by EU-US Privacy Shield framework. Both of VouchedFor's suppliers are registered under the Privacy Shield framework. |

If you would like further information regarding our data transfers and the steps we take to safeguard your personal information, please contact a member of the HR team or the Data Protection Officer.

## What are my rights in relation to my personal data?

The Company will always seek to process your personal data in accordance with its obligations and your rights.

You will not be subject to decisions based solely on automated data processing without your prior consent.

In certain circumstances, you have the right to seek the erasure or correction of your personal data, to object to particular aspects of how your data is processed, and otherwise to seek the restriction of the processing of your personal data. You also have the right to request the transfer of your personal data to another party in a commonly used format. If you have any questions about these rights, please contact the Data Protection Officer using the details set out below.

You have a separate right of access to your personal data processed by the Company. You may be asked for information to confirm your identity and/or to assist the Company to locate the data you are seeking as part of the Company's response to your request. If you wish to exercise your right of access you should set out your request in writing to the Data Protection Officer using the details set out below.

Finally, you have the right to raise any concerns about how your personal data is being processed with the Data Protection Commissioner's Office by going to their website https://www.dataprotection.ie/docs/Making-a-Complaint-to-the-Data-Protection-Commissioner/r/18.htm or info@dataprotection.ie

## Where can I get further information?

The Company has appointed a Data Protection Officer to oversee compliance with this Notice and to deal with any questions or concerns. If you would like further information about the matters set out in this Notice, please contact a member of the HR team or the Data Protection Officer.

The contact details for the Data Protection Officer are set out below:

**Data Protection Officer:**
John Sheehan
compliance@ecclesiastical.com

*Please sign below indicating that you have read and understood the employee privacy notice and that you consent to the processing of your personal data as detailed.*

Print Name: _____

Signature:_____ Date: _____