



DATA PROTECTION AND PRIVACY NOTICE

Ecclesiastical is committed to the privacy and confidentiality of information that you provide to us. This data protection and privacy notice describes our current policies and practices with regard to personal information collected and used by us.

Please take your time to read this notice carefully. When using Ecclesiastical websites (namely ecclesiastical.com, benefactgroup.com and Movementforgood.com), this notice should be read alongside the [website terms and conditions](#).

Contents:

- 1 About us
- 2 About the insurance market
- 3 Our processing of your personal information
 - 3.1 Prospective policyholder or beneficiary under an insurance policy
 - 3.2 Policyholder or beneficiary under an insurance policy
 - 3.3 Third party claimant
 - 3.4 Third party pursued for a recovery
 - 3.5 Witness to an incident
 - 3.6 Brokers, appointed representatives, financial adviser and other business partners
 - 3.7 Applications for grants & bursaries
 - 3.8 Users of the Ecclesiastical websites.
- 4 How will we use your personal data for marketing?
- 5 Automated Decision-Making, Profiling and Artificial Intelligence (AI)
- 6 How long do we keep personal information for?
- 7 What is our approach to sending your personal information
- 8 How do we protect your information?
- 9 Your rights
- 10 Contacting us
- 11 Updates to this notice

1. About us

Ecclesiastical Insurance Office plc ("EIO", "Ecclesiastical", "we", "us" or "our") is committed to protecting the privacy, confidentiality and security of the personal information entrusted to us.

This Privacy Notice explains how we collect, use, disclose, retain and protect personal information relating to individuals who interact with us, including prospective customers, policyholders, beneficiaries, claimants, witnesses, business partners, grant applicants and users of our websites. It also explains the rights available to individuals under the General Data Protection Regulation ("GDPR"), the Data Protection Act 2018 and other applicable Irish and European data protection laws.

Ecclesiastical Insurance Office plc is a specialist insurer providing insurance products and associated services to faith organisations, charities, educational institutions, heritage properties, property owners, businesses and private individuals. We are part of the Benefact Group.

For the purposes of the GDPR, Ecclesiastical Insurance Office plc is the **Data Controller** of the personal information described in this Privacy Notice unless otherwise stated. This means we determine the purposes for which and the manner in which your personal information is processed.

Ireland Branch

Ecclesiastical Insurance Office plc operates in Ireland through its registered Irish branch:

Ecclesiastical Insurance Office plc

4th Floor, The Heysham
73 North Wall Quay
Dublin, D01 V2F4
Ireland

Telephone: +353 (0)1 619 0300

Website: www.ecclesiastical.ie

Contacting Our Data Protection Team

If you have any questions regarding this Privacy Notice, wish to exercise your data protection rights, or would like further information about the way we process your personal data, you may contact our Data Protection Officer using the details below:

Data Protection Officer

Ecclesiastical Insurance Office plc
4th Floor, The Heysham
73 North Wall Quay
Dublin, D01 V2F4
Ireland

Email: **ComplianceIreland@ecclesiastical.com**

We encourage individuals to contact us first so that we can attempt to resolve any queries or concerns regarding the processing of personal information promptly and effectively

Data Protection Commission

The Data Protection Commission is Ireland's supervisory authority for data protection matters.

Website: www.dataprotection.ie

You have the right to lodge a complaint with the Data Protection Commission if you believe your personal information has been processed in breach of applicable data protection law.

Our Regulatory Environment

As an insurance undertaking, we are subject to various legal, regulatory and professional obligations. These obligations require us to collect, use and retain personal information to:

- provide insurance quotations;
- assess and underwrite insurance risk;
- administer insurance policies;
- investigate, manage and settle claims;
- prevent, detect and investigate fraud and financial crime;
- comply with legal and regulatory requirements;
- defend or pursue legal claims; and
- manage and improve our business operations.

Benefact Group

Ecclesiastical Insurance Office plc forms part of the Benefact Group, a group of companies operating in insurance, financial services, charitable giving and related activities.

In some circumstances, we may share personal information with other companies within the Benefact Group where there is a lawful basis for doing so and where such sharing is necessary for administrative, operational, regulatory, governance, risk management, audit, customer service or business continuity purposes. Any such sharing will take place in accordance with applicable data protection laws and appropriate safeguards.

Scope of this Privacy Notice

This Privacy Notice applies to personal information relating to:

- prospective policyholders and beneficiaries;
- policyholders and insured persons;
- claimants and third parties involved in claims;
- individuals pursued as part of recovery or subrogation actions;
- witnesses to insured incidents;
- brokers, intermediaries and business partners;
- applicants for grants or bursaries;
- users of our websites and digital services; and

any other individual whose personal information we process in connection with our insurance activities. Providing insurance services requires us to process personal information. Without certain personal information, we may be unable to provide quotations, arrange insurance cover, administer policies, manage claims or comply with our legal and regulatory obligations.

2. About the insurance market

Insurance involves the use and disclosure of personal information by a range of insurance market participants including intermediaries, brokers, insurers, reinsurers, claims handlers, professional advisers and regulatory authorities. Personal information may be exchanged between these parties where necessary for the provision of insurance products and services, the administration of policies, the handling of claims, the prevention and detection of fraud, and compliance with legal and regulatory obligations.

As part of providing insurance services, we may receive personal information from, and share personal information with, other insurance market participants where we have a lawful basis to do so. This may include information relating to insurance applications, policy administration, claims handling, complaints, fraud prevention, recovery actions and legal proceedings.

Where personal information is transferred within the insurance market, we take reasonable steps to ensure that such processing is carried out in accordance with the GDPR, the Data Protection Act 2018 and applicable

regulatory requirements.

3. Our processing of your personal information

Depending on our relationship with you and the nature of the services we provide, we will collect different types of personal information and use it for different purposes. This may include information relating to policyholders, beneficiaries, claimants, witnesses, brokers, business partners, grant applicants and users of our websites

In certain circumstances, we may also collect and process **Special Category Personal Data** (formerly referred to as sensitive personal data) and information relating to criminal convictions and offences where this is necessary for insurance purposes, claims handling, fraud prevention, compliance with legal obligations or the establishment, exercise or defence of legal claims. This may include information relating to health, religious or philosophical beliefs, or criminal convictions and offences where relevant to the services we provide.

Where you provide us with personal information about another individual, such as a family member, beneficiary, employee, trustee, volunteer or other insured person, we may also process that individual's personal information in accordance with this Privacy Notice. You should ensure that any such individual is made aware of this Privacy Notice and the way in which we may process their personal information.

We have structured this Privacy Notice so that you can refer to the section that is most relevant to your relationship with us. The following sections explain the personal information we collect, how we collect it, how we use it, the lawful bases on which we rely, and the parties with whom we may share it.

Where we obtain personal information indirectly from third parties rather than directly from you, we will provide privacy information in accordance with Article 14 GDPR unless an exemption applies.

3.1 Prospective policyholder or beneficiary under an insurance policy

If you apply for an insurance policy with us (for example, a home insurance policy), or someone applies for a policy which will cover you or list you as a named beneficiary (for example, a clergy member under a church legal expenses insurance policy), this section will be applicable to you and will provide key information about how we use your personal information.

3.1.1 What personal information will we collect?

If you apply for an insurance policy with us, or if someone applies for a policy which covers you or identifies you as a beneficiary, we may collect the following categories of personal information: Your name, title, postal address, telephone number(s), email address, date of birth and gender

Where you are not the person applying for insurance, information regarding your relationship to, or connection with, the prospective policyholder.

- Identity and verification information where required, including documentation used to verify your identity and comply with legal and regulatory obligations, such as passport details, driving licence details, PPS Number, change of name documentation, executorship details or other verification documentation.
- Employment and occupation information, including your employment status, occupation, employer details, employment history and, where relevant, educational background.
- Information relating to your insurance application, including:
 - details of previous insurance policies;
 - details of previous claims or losses;
 - information relating to family members, dependents, beneficiaries or other people insured under the policy; and
- information relevant to the specific insurance product for which you are applying. For example, this may include information about your property, contents, valuables, collections, charity activities, church activities, educational premises or other insured risks
- Financial information, including:
 - bank account details and payment information;
 - information about your income where relevant to the insurance product;
 - information obtained as part of sanctions, anti-money laundering, fraud prevention or financial checks; and
- information relating to insolvency proceedings, bankruptcy, court judgments or other legally reportable financial matters where relevant.
- Information available from publicly accessible sources where relevant to the assessment of an insurance application, the prevention of fraud or compliance with legal and regulatory obligations. This may include information obtained from public registers, court records, insolvency registers, internet searches or publicly available directories.
- Information that helps us identify whether you may require additional support or assistance when engaging with us, so that we can provide our services in an appropriate and fair manner.

3.1.2 What sensitive personal information will we collect?

- In certain circumstances, we may collect and process **Special Category Personal Data** and information relating to criminal convictions and offences where this is necessary to provide insurance services, assess risk, administer a policy, handle a claim, prevent fraud, comply with legal obligations or exercise legal rights. We process personal data relating to criminal convictions and offences only where authorised by applicable law and subject to appropriate safeguards designed to protect the rights and freedoms of individuals.

- This may include:
- Information relating to your physical or mental health, medical conditions, disabilities or vulnerabilities where relevant to your application for insurance or the cover requested. For example, where you apply for a travel insurance policy, we may require details of pre-existing medical conditions.
- Information relating to criminal convictions, criminal offences, alleged offences, sanctions, court orders or other information relevant to the prevention, detection and investigation of fraud, financial crime or other unlawful activity.
- Information that reveals or may reveal your racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sexual orientation or other Special Category Personal Data where such information is relevant to the insurance product, risk assessment or policy administration. For example, where you are identified as a member of the clergy or hold a role within a faith-based organisation, information relating to your religious beliefs may be inferred from the information provided to us.
- Information that assists us in identifying customers who may require additional support or assistance when engaging with us, where such information includes Special Category Personal Data.
- We will only collect and use Special Category Personal Data and information relating to criminal convictions and offences where we have identified an appropriate lawful basis under the GDPR and applicable Irish law, including where processing is necessary for insurance purposes, compliance with legal obligations, the establishment, exercise or defence of legal claims, substantial public interest purposes permitted by law, or where you have provided your explicit consent.

3.1.3 How will we collect your personal information?

We may collect your personal information directly from you, from the prospective policyholder, from insurance market participants and from other third parties who assist us in providing insurance services.

Directly from you:

- when you request a quotation;
- when you apply for an insurance policy;
- when you communicate with us by telephone, email, post, online forms or through our website; and
- when you make an enquiry, submit documentation or provide information in support of an insurance application.

We may also collect your personal information from:

- the prospective policyholder where you are a beneficiary or are otherwise connected to the insurance application;
- insurance intermediaries, brokers, insurers, reinsurers and other insurance market participants involved in the provision or administration of insurance services;
- third parties who provide sanctions screening, identity verification, anti-money laundering and fraud prevention services;
- fraud prevention agencies, financial crime databases and organisations that maintain fraud prevention and detection registers;
- other companies within the Benefact Group where there is a lawful basis to share information;
- publicly available sources, including court judgments, insolvency registers, regulatory registers, internet searches and publicly available directories where relevant to the assessment of risk, fraud prevention or compliance with legal and regulatory obligations; and service providers and other third parties who assist us in verifying information or administering insurance services.
- Fraud prevention databases, sanctions screening providers, anti-money laundering service providers, credit reference agencies and identity verification service providers where relevant and legally permitted.

Where we obtain personal information from a third party, we will process that information in accordance with applicable data protection laws and this Privacy Notice.

3.1.4 What will we use your personal information for?

We use your information in a number of different ways, depending on your circumstances. For every use, we must be able to demonstrate that there is a legal basis for doing so.

When using your personal information, we will rely on one or more of the following legal bases:

- **It is necessary to enter into or perform an insurance contract.** We rely on this legal basis for activities connected with assessing your application, providing quotations, arranging cover and administering insurance products.
- **It is necessary to comply with a legal obligation.** This includes complying with anti-money laundering requirements, financial crime prevention measures, regulatory record-keeping obligations, responding to requests relating to your data protection rights and reporting obligations imposed by law.
- **It is necessary for our legitimate interests or those of a third party.** This includes fraud prevention, business administration, identifying customers who may require additional support, maintaining management information, improving our products and services, carrying out statistical analysis and ensuring the effective operation of our business. Where we rely on legitimate interests, we will ensure that our interests are not overridden by your rights and freedoms.
- **You have provided your consent.** Where consent is required by law, including certain marketing activities, we will rely on your consent and you may withdraw that consent at any time.

When we use Special Category Personal Data or information relating to criminal convictions and offences, we will rely on one or more of the following additional legal bases:

- **Processing is necessary for reasons of substantial public interest**, in accordance with Article 9(2)(g) GDPR and applicable Irish law.
- **Processing is necessary for the establishment, exercise or defence of legal claims**, in accordance with Article 9(2)(f) GDPR.
- **You have manifestly made the personal data public**, in accordance with Article 9(2)(e) GDPR.
- **You have provided your explicit consent**
- **Processing is necessary for insurance purposes where permitted under applicable Irish law and appropriate safeguards are in place**

3.1.5 What are the legal grounds on which we will use your personal information?

What is the purpose for using your personal information?	Legal grounds for using your personal information	Legal grounds for using your sensitive personal information
Assessing your insurance application.	• Performance of a Contract • Compliance with a Legal Obligation • Legitimate Interests (preventing fraud, money laundering and other financial crime)	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest • Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims
Carrying out medical screening for travel insurance policies.	• Performance of a Contract • Compliance with a Legal Obligation • Legitimate Interests (preventing fraud, money laundering and other financial crime)	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest
Carrying out fraud, credit and anti-money laundering checks on you.	• Performance of a Contract • Compliance with a Legal Obligation • Legitimate Interests (preventing fraud, money laundering and other financial crime)	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest • Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims
Complying with our legal or regulatory obligations, including detecting unlawful acts, responding to personal data breaches or dealing with requests relating to your data protection rights.	• Compliance with a Legal Obligation • Legitimate Interests (ensuring effective compliance and governance)	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest • Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims
Identifying individuals who may require additional support.	• Legitimate Interests (to ensure customers are treated fairly and receive appropriate support)	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest
Generally communicating with you and handling any queries or complaints about your application.	• Performance of a Contract • Compliance with a Legal Obligation • Legitimate Interests (to manage communications and resolved complaints)	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest • Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims • Information Manifestly Made Public by You (where applicable)

Business purposes such as systems development, migration of systems, diagnosis of technical issues, improving business efficiency, internal audits, analysing sales and usage of our services and products.	• Legitimate Interests (to operate, develop and improve our business and services)	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest (where Special Category Personal Data is processed)
Providing improved quality, training and security (for example, through recorded or monitored telephone calls to our contact numbers or carrying out customer satisfaction surveys).	• Legitimate Interests (to monitor, review and improve our products, services, customer experience, training and security arrangements)	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest where Special Category Personal Data is incidentally disclosed during monitored communications • Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims (where applicable)
Contacting you about products and services that may be of interest to you.	• Consent • Legitimate Interests (where permitted under applicable Irish ePrivacy legislation)	• Explicit Consent

3.1.6 Who will we share your personal information with?

We will only share your personal information where necessary and where we have an appropriate legal basis for doing so.

We may share your personal information with:

- The policyholder, where you are a beneficiary under the policy.
- Insurance intermediaries, brokers, insurers, reinsurers and other insurance market participants involved in the assessment, administration or servicing of your insurance application.
- Third-party service providers who assist us in administering insurance products and services, including claims service providers, medical screening providers, professional advisers and specialist consultants.
- Third parties who provide identity verification, sanctions screening, anti-money laundering, fraud prevention and financial crime detection services.
- Fraud prevention agencies and organisations that maintain fraud prevention, fraud detection and financial crime databases.
- Other companies within the Benefact Group, where there is a legitimate interest to share information and such sharing is permitted by applicable data protection laws.
- Service providers engaged by us, including subcontractors, agents, auditors, solicitors, actuarial advisers, IT service providers, cloud service providers, database providers, document management providers and other business suppliers.
- Professional advisers, including legal advisers, auditors and consultants where disclosure is necessary for the provision of professional services or the protection of our legal interests.
- Regulatory authorities, supervisory bodies and public authorities where disclosure is required or permitted by law.
- Law enforcement agencies, courts, tribunals, government bodies, the Revenue Commissioners or other competent authorities where we are legally required or permitted to do so.
- Any person or organisation involved in the sale, transfer, merger, restructuring or reorganisation of all or part of our business, provided appropriate confidentiality and data protection safeguards are in place.
- Our insurers, reinsurers and service providers engaged to assist with arranging, managing or administering our own insurance arrangements.

Where personal information is shared with third parties, we take reasonable steps to ensure that appropriate contractual, technical and organisational measures are in place to protect your personal information and to ensure that it is processed in accordance with applicable data protection laws.

3.2 Policyholder or beneficiary under an insurance policy

If you have an insurance policy with us (for example, home insurance policy), if the policy covers you or if you are a named individual under an insurance policy with us (for example, a clergy member under a church legal expenses insurance policy), this section will be applicable to you and will provide key information about how we use your personal information. We process personal data relating to criminal convictions and offences only where authorised by applicable law and subject to appropriate safeguards designed to protect the rights and freedoms of individuals.

3.2.1 What personal information will we collect?

- Your name and title, address, telephone numbers and email addresses, date of birth and gender.
- Where you are not the policyholder, your relationship or connection to the policyholder.
- Identity information if necessary, including marriage certificate, change of name documentation, PPS number, executorship details, and documents such as passport and driving licence.
- Employment status and related information such as job title, employment history and education.
- Information which is related to your insurance policy including:
 - details about previous insurance policies you have held and any previous claims you have made;
 - details about your family such as dependants or spouses; and
 - policy specific information. For example, if you have home insurance, we will need information about your property and possessions or where you hold an art and private client policy, we will need information about your art collection.
- Financial information including:
 - your bank account and payment details;
 - details about your income; and
 - information obtained from checking sanctions lists and credit checks such as bankruptcy orders, individual voluntary arrangements, office disqualifications or county court judgments.
- Information which is relevant to any claims you make under your policy. This could include photographic evidence you provide us with.
- Information which is available publicly such as internet search engines and social media where we need to investigate fraudulent claims.
- Security questions and answers to access the Ecclesiastical portal where policy documents can be viewed.
- Information to assist us with determining whether you require additional support.

3.2.2 What Special Category Personal Data will we collect?

- Information about your physical and mental health, including information that may indicate you require additional support when engaging with us, and if relevant to your insurance policy or any claims you make (for example, on sickness or accident policies or where you take out a travel policy and make a claim for medical assistance, we will need information about the medical conditions suffered. This information may be provided to us in the form of GP reports or medical data such as blood tests).
- Information about any criminal offences you have been convicted of and any related information including about any offences or alleged offences you have committed or any court sentences which you are subject to. Where we process personal data relating to criminal convictions and offences, we do so only where permitted by Article 10 GDPR, the Data Protection Act 2018 and other applicable Irish law and subject to appropriate safeguards.
- We may also collect information because it is relevant to your policy or claim, which reveals or is likely to reveal your race or ethnicity, religious or philosophical beliefs; political opinions; trade union membership; or data concerning your sex life or sexual orientation. For example, where we process information about you because you are a clergy member at an Anglican Church, this will automatically reveal your religious beliefs.

3.2.3 How will we collect your personal information?

When you are the policyholder, directly from you:

- when we provide you with a quote;
- when you apply for or renew a policy;
- when you make a claim on your policy; and
- during any communications we have, such as by telephone or email or when you make a complaint or general enquiry.

We will also collect your personal information from:

- The policyholder where you are a beneficiary.
- A third party who has power of attorney over you.
- Third parties who we rely on to administer insurance and handle claims such as brokers, insurers, third party claimants, defendants, witnesses and our own business partners.
- Third parties we (or you) appoint to assist with an insurance policy or claim such as claims handlers, medical experts and medical screening service providers, investigators and loss adjusters. This may include claims management service providers such as Kennedys IQ Limited. Where such organisations act as joint controllers or independent controllers, further information regarding the arrangement will be made available upon request.
- Third parties who provide fraud detection and investigation, and sanctions checking services.
- Financial crime and fraud detection agencies and other third parties who operate and maintain fraud detection registers and third parties we use to carry out credit checks, who will be a Joint Data Controller together with EIO and other contributing organisations.
- Other companies in the Benefact Group.
- Public sources such as court judgments, insolvency registers, internet search engines, social media where we need to investigate fraudulent claims and directories of Anglican ministers.
- Fraud prevention databases, sanctions screening providers, anti-money laundering service providers, credit reference agencies and identity verification service providers where relevant and legally permitted.
- Regulatory authorities, supervisory bodies and other competent authorities where disclosure is required or permitted by law.

3.2.4 What will we use your personal information for?

We use your information in a number of different ways, depending on your circumstances. For every use, we must be able to demonstrate that there is a “legal ground” to do so. When using your “personal information”, we will rely on one or more of the following legal bases:

- **Performance of a Contract.** We use your personal information where necessary to provide insurance cover, administer your policy, handle claims and deliver the services requested by you.
- **Compliance with a Legal Obligation.** We may process your personal information where necessary to comply with legal and regulatory obligations, including anti-money laundering requirements, fraud prevention obligations, regulatory reporting obligations and responding to requests relating to your data protection rights.
- **Legitimate Interests.** We may process your personal information where necessary for our legitimate interests, including fraud prevention, business administration, improving our products and services, maintaining records and identifying customers who may require additional support.
- **Consent.** We may process your personal information where you have provided your consent, including certain marketing activities and where consent is required under applicable Irish ePrivacy legislation.

When we use Special Category Personal Data or information relating to criminal convictions and offences, we will rely on one or more of the following additional legal bases:

- Processing is necessary for reasons of substantial public interest in accordance with Article 9(2)(g) GDPR and applicable Irish law.
- Processing is necessary for the establishment, exercise or defence of legal claims in accordance with Article 9(2)(f) GDPR.
- You have manifestly made the personal data public in accordance with Article 9(2)(e) GDPR.
- You have provided your explicit consent in accordance with Article 9(2)(a) GDPR.

3.2.5 What are the legal grounds on which we will use your personal information?

What is the purpose for using your personal information?	Legal grounds for using your personal information	Legal grounds for using your sensitive personal information
To provide an insurance policy with appropriate cover.	• Performance of a Contract • Legitimate interest (to provide insurance cover which is in line with our own risk appetite).	• Article 9(2)(g) GDPR – Substantial Public Interest • Manifestly Made Public (where applicable)
To carry out medical screening for travel insurance policies.	• Performance of a Contract • Legitimate interest (to carry out medical screening to ensure that we provide appropriate insurance cover)	• Article 9(2)(g) GDPR – Substantial Public Interest
To handle any claims you make under your insurance policy.	• Performance of a Contract • Legitimate interest (to investigate claims, respond and conclude all claims)	• Article 9(2)(f) GDPR – Establishment, Exercise or Defence of Legal Claims • Manifestly Made Public (where applicable)
To carry out fraud, credit and anti- money laundering checks on you when you enter into a policy and to prevent any fraudulent claims.	• Performance of a Contract • Compliance with a legal obligation. • Legitimate interest (to prevent fraud and other financial crime).	• Article 9(2)(f) GDPR – Establishment, Exercise or Defence of Legal Claims • Article 9(2)(g) GDPR – Substantial Public Interest
To comply with our legal or regulatory obligations including, for example, detecting unlawful acts or dishonesty, responding to personal data breaches or requests relating to your data protection rights.	• Compliance with a legal obligation. • Legitimate Interests (to respond to all communications).	• Article 9(2)(g) GDPR – Substantial Public Interest
To identify individuals who may require additional support.	• Legitimate interest (to ensure individuals are treated fairly).	• Article 9(2)(g) GDPR – Substantial Public Interest and applicable provisions of the Data Protection Act 2018 relating to insurance and vulnerable customers.

To handle any complaints, you may have and generally communicate with you.	• Compliance with a legal obligation. • Performance of a Contract • Legitimate Interests (to respond to all communications and to investigate and resolve complaints).	• Article 9(2)(f) GDPR - Establishment, Exercise or Defence of Legal Claims • Article 9(2)(g) GDPR - Substantial Public Interest • Manifestly Made Public
To pursue or defend legal claims.	• Legitimate Interests (to pursue or defend legal claims) • Compliance with a legal obligation.	• Article 9(2)(f) GDPR - Establishment, Exercise or Defence of Legal Claims
To apply for and claim on our own insurance.	• Legitimate interest (to have our own insurance cover in place). • Legitimate interests (to make or manage claims under our insurance policies).	• Article 9(2)(f) GDPR - Establishment, Exercise or Defence of Legal Claims. • Article 9(2)(g) GDPR - Substantial Public Interest (where processing is necessary for insurance purposes under applicable law).
For business purposes such as systems development migration of systems, diagnosing any problems with our servers and website, improving the efficiency of our business, performing internal audits, analysing sales and usage of our services and products.	• Legitimate interest (to operate, maintain and improve our business and systems).	• Article 9(2)(g) GDPR - Substantial Public Interest (where processing is necessary for insurance administration purposes). We do not generally use sensitive personal information for systems development activities unless strictly necessary and subject to appropriate safeguards. •
For financial purposes such as maintaining management information and accounting records.	• Legitimate interests (to maintain appropriate financial records). • Compliance with a legal obligation	• Article 9(2)(g) GDPR - Substantial Public Interest. • Compliance with legal and regulatory obligations.
To provide improved quality, training and security (for example, through recorded or monitored phone calls to our contact numbers or carrying out customer satisfaction surveys).	• Legitimate interests (to develop and improve the services we offer).	• Article 9(2)(g) GDPR - Substantial Public Interest (where sensitive personal information is incidentally included in communications).
To contact you to inform you about services we think you might be interested in.	• Legitimate Interests (to inform you about other services we offer) • We have your consent.	• Article 9(2)(a) GDPR - Explicit Consent.

3.2.6 Who will we share your personal information with?

We will only share your personal information where necessary for the purposes set out in this Privacy Notice and where we have an appropriate legal basis for doing so.

We may share your personal information with:

- The policyholder, where you are a beneficiary or a person insured under the policy.
- A person acting on your behalf, including an attorney acting under an Enduring Power of Attorney, legal representative, executor, administrator or another authorised representative.
- Insurance intermediaries, brokers, insurers, reinsurers and other insurance market participants involved in the provision, administration, renewal or servicing of your insurance policy.
- Third parties whom we or you appoint to assist in connection with a policy or claim, including claims handlers, medical experts, medical screening providers, surveyors, investigators, loss adjusters, engineers, valuers and recovery specialists.
- Third-party service providers who assist us in underwriting insurance risks, administering policies, handling claims, managing complaints and providing customer support.
- Third parties who provide identity verification, sanctions screening, anti-money laundering, fraud prevention, fraud detection and financial crime monitoring services.
- Fraud prevention agencies and organisations which maintain fraud prevention and fraud detection databases and registers.
- Professional advisers including solicitors, barristers, auditors, accountants, actuaries, consultants and other specialist advisers where disclosure is necessary for the provision of professional services or the protection of our legal interests.
- Other companies within the Benefact Group where there is a legitimate interest in information sharing and such sharing is carried out in accordance with applicable data protection laws.
- Service providers engaged by us, including subcontractors, agents, IT service providers, cloud service providers, database providers, document management providers, communication providers and other business suppliers who support the delivery of our services.
- Regulatory authorities, supervisory bodies and public authorities where disclosure is required or permitted by law or regulatory requirements.
- The Data Protection Commission, the Central Bank of Ireland and other competent regulatory or supervisory authorities where disclosure is required by law or necessary for regulatory purposes.
- Law enforcement agencies, courts, tribunals, government departments, the Revenue Commissioners and other public authorities where disclosure is required or permitted by law.
- Any third party involved in the sale, merger, acquisition, restructuring, transfer or reorganisation of all or part of our business, provided appropriate confidentiality and data protection safeguards are in place.
- Our own insurers, reinsurers and service providers appointed to assist with arranging, managing or administering our own insurance arrangements.

Where we share personal information with third parties, we take reasonable steps to ensure that appropriate contractual, technical and organisational measures are in place to protect personal information and to ensure that it is processed in accordance with applicable data protection legislation.

3.3 Third party claimant

If you make a claim against a third party who has an insurance policy with us, this section will be applicable to you and will provide key information about how we use your personal information.

3.3.1 What personal information will we collect?

- Your name and title, address, telephone numbers and email addresses, date of birth and gender
- Identity information such as PPS number.
- Any information which is related to your claim which could include:
 - your job title and employment status, employment history, salary and education if relevant;
 - details about the incident; and
 - supporting evidence.
- Information which is available publicly such as via internet search engines and social media where we need to investigate potentially fraudulent claims.
- Information to assist us with determining whether you require additional support.

3.3.2 What Special Category Personal Data Will We Collect?

- Information relating to your physical or mental health, including any medical conditions, injuries, treatment, prognosis, rehabilitation requirements or additional support needs, where relevant to the claim you are making.
- Information relating to criminal convictions and offences where relevant to the assessment, investigation, defence or settlement of a claim. We process personal data relating to criminal convictions and offences only where authorised by applicable law and subject to appropriate safeguards designed to protect the rights and freedoms of individuals.
- Information that may reveal your racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, sex life or sexual orientation where such information is relevant to the claim, legal proceedings or valuation of the claim.

3.3.3 How will we collect your personal information?

Directly from you when you contact us to make a claim.

We will also collect your personal information from:

- The policyholder.
- Third parties who we rely on to provide insurance and handle claims such as brokers, insurers, third party claimants, defendants, witnesses and our own business partners.
- Third parties we appoint to assist with a claim such as claims handlers, medical experts we have commissioned to produce a medical report and medical screening service providers, investigators and loss adjusters.
 - Third parties involved in the claim process such as lawyers or the Irish Courts
 - Third parties who provide fraud detection and investigation, and sanctions checking services.
 - Financial crime and fraud detection agencies and other third parties who operate and maintain fraud detection registers and third parties we use to carry out credit checks.
 - Public sources such as court judgments, insolvency registers, internet search engines, social media
 - The Central Bank of Ireland who is our regulator.
 - Fraud prevention databases, sanctions screening providers, anti-money laundering service providers, credit reference agencies and identity verification service providers where relevant and legally permitted.

3.3.4 What Will We Use Your Personal Information For?

We use your information in a number of different ways, depending on your particular circumstances. For every use, we must be able to demonstrate that there is a legal basis for doing so.

When we use your personal information, we will rely on one or more of the following legal bases:

- Compliance with a Legal Obligation. Such obligations include maintaining appropriate records, preventing and detecting fraud and financial crime, responding to requests relating to your data protection rights, complying with regulatory requirements and responding to personal data breaches.
- Legitimate Interests. These interests include investigating and assessing claims, handling and resolving disputes, defending legal proceedings, exercising rights of recovery or subrogation, maintaining business records, improving our services, carrying out statistical analysis and ensuring the effective operation of our business.

When we use Special Category Personal Data or information relating to criminal convictions and offences, we will rely on one or more of the following additional legal bases:

- Processing is necessary for reasons of substantial public interest, in accordance with Article 9(2)(g) GDPR and applicable Irish law.
- Processing is necessary for the establishment, exercise or defence of legal claims, in accordance with Article 9(2)(f) GDPR.
- You have manifestly made the personal data public, in accordance with Article 9(2)(e) GDPR.
- You have provided your explicit consent, in accordance with Article 9(2)(a) GDPR.

3.3.6 What are the legal grounds on which we will use your personal information?

What is the purpose for using your personal information?	Legal grounds for using your personal information	Legal grounds for using your sensitive personal information
To handle your claim.	• Compliance with a Legal Obligation • Legitimate Interests (to ensure effective compliance, governance and risk management)	• Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims
To carry out fraud checks and prevent fraudulent claims.	• Legitimate Interests (fraud prevention and protection of policyholders, customers and the wider insurance market) • Compliance with a Legal obligation	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest - Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims
To comply with our legal or regulatory obligations including, for example, detecting unlawful acts or dishonesty, responding to personal data breaches or requests relating to your data protection rights.	• Compliance with a Legal Obligation	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest - Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims
To handle any complaints, you may have and generally communicate with you and your medical/legal representatives.	• Legitimate Interests (to investigate, manage and resolve claims and complaints)	• Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims - Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest
To pursue or defend legal claims and rights, including exercising our right of subrogation (that is to bring an action for recovery of the claim amount we have paid against the third party who we believe caused the loss or injury).	• Legitimate Interests (to pursue, defend and enforce legal rights and recover losses where appropriate) • Compliance with a legal obligation.	• Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims
To apply for and claim on our own insurance.	• Legitimate Interests (to maintain appropriate insurance protection for our business) legitimate interest	• Article 9(2)(f) GDPR - Processing necessary for the establishment, exercise or defence of legal claims

For business purposes such as systems development, migration of systems, diagnosing any problems with our servers and website, improving the efficiency of our business, performing internal audits, analysing usage of our services and products	• Legitimate Interests (to operate, improve and develop our business and services) legitimate interest	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest (where Special Category Personal Data is processed)
For financial purposes such as maintaining management information and accounting records.	• Compliance with a Legal Obligation Legitimate Interests (to maintain appropriate financial records and controls) legitimate interest	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest
To provide improved quality, training and security (for example, through recorded or monitored phone calls to our contact numbers or carrying out customer satisfaction surveys).	• Compliance with a Legal Obligation Legitimate Interests (to maintain appropriate financial records and controls) legitimate interest	• Article 9(2)(g) GDPR - Processing necessary for reasons of substantial public interest

3.3.7 Who will we share your personal information with?

We will only share your personal information where necessary for the purposes described in this notice, where we have a lawful basis under Article 6 GDPR and, where applicable, a condition under Article 9 GDPR or Article 10 GDPR. We do not sell your personal information.

We may share your personal information with:

- The policyholder and other insurers, reinsurers, brokers or intermediaries involved in the claim.
- Claims handlers, loss adjusters, investigators, surveyors, medical experts and other professional advisers engaged to assess, investigate or settle the claim.
- Solicitors, barristers, courts, tribunals, mediators and other parties where necessary to establish, exercise or defend legal claims.
- Witnesses, defendants, recovery targets and their legal representatives where necessary for the investigation, defence or resolution of a claim.
- Fraud prevention agencies, sanctions screening providers and organisations involved in the prevention, detection and investigation of fraud, money laundering or other criminal activity.
- Regulatory authorities, supervisory authorities and public bodies, including the Central Bank of Ireland, the Data Protection Commission, An Garda Síochána, the Revenue Commissioners, courts and other competent authorities where disclosure is required by law.
- Service providers acting on our behalf, including IT, cloud hosting, document management, audit and administrative support providers. Where they act as processors, they are subject to contracts meeting the requirements of Article 28 GDPR.
- Other companies within the Benefact Group where necessary for claims administration, fraud prevention, information security, internal audit, regulatory compliance or business continuity purposes.
- Our auditors, insurers and professional advisers.
- Prospective purchasers, merger partners or successor organisations in connection with a corporate transaction, subject to appropriate confidentiality obligations.

Where special category data or criminal offence data is disclosed, we will do so only where permitted by applicable EU or Irish law and subject to appropriate safeguards.

In some circumstances, we may act as a joint controller with another organisation. Where this occurs, we will comply with Article 26 GDPR and make the essence of the arrangement available on request.

Where personal data is transferred outside the European Economic Area (EEA), we will ensure appropriate safeguards are in place, including adequacy decisions, Standard Contractual Clauses, Binding Corporate Rules or other transfer mechanisms recognised under Chapter V GDPR.

We will only share the minimum personal information necessary for the relevant purpose and will ensure recipients are subject to appropriate confidentiality and security obligations.

3.4 Third party pursued for a recovery

If you are a third party from whom we are seeking recovery when we exercise our right of subrogation, this section will be applicable to you and will provide key information about how we use your personal information. We may exercise this right where we have paid a claim under an insurance policy, but we believe that your act or failure to act caused the loss or injury.

3.4.1 What personal information will we collect?

- Your name and title, address, telephone number and email address, date of birth and gender;
- Any information which is related to the relevant claim which could include:
 - your job title and employment status, employment history and salary and education if relevant;
 - details about the incident and your actions; and
 - photographic evidence.
- Information which is available publicly such as via internet search engines and social media.

3.4.2 What sensitive personal information will we collect?

- Information about your physical and mental health if relevant to the claim.
- Information about any criminal offences you have been convicted of and any related information including about any offences or alleged offences you have committed or any court sentences which you are subject to. We process personal data relating to criminal convictions and offences only where authorised by applicable law and subject to appropriate safeguards designed to protect the rights and freedoms of individuals.
- We may also collect information because it is relevant to the claim made under an Ecclesiastical policy, which reveals or is likely to reveal your; race or ethnicity, religious or philosophical beliefs, political opinions, trade union membership, or data concerning your sex life or sexual orientation.

3.4.3 How will we collect your personal information?

We will collect your personal information from:

- The policyholder.
- Third parties who we rely on to provide insurance and handle claims such as brokers, insurers, third party claimants, witnesses and our own business partners.
- Third parties we appoint to assist with a claim such as claims handlers, investigators and loss adjusters.
- Third parties involved in the claim process such as lawyers or the Irish Courts
- Public sources such as court judgments, internet search engines and social media
- Fraud prevention databases sanctions screening providers, anti-money laundering service providers, credit reference agencies and identity verification service providers where relevant and legally permitted.

3.4.4 What will we use your personal information for?

We use your personal information for a number of purposes relating to the investigation, assessment and handling of insurance claims. For each use of your personal information, we must identify a lawful basis under applicable data protection law.

When using your personal information, we may rely on one or more of the following legal bases:

- **Compliance with a legal obligation**, including obligations relating to fraud prevention, regulatory compliance, financial crime prevention, record keeping, responding to data protection requests, and communicating with regulatory or law enforcement authorities.
- **Our legitimate interests**, including investigating and managing claims, preventing fraud, exercising or defending legal rights, maintaining business records, improving our services, operating our business efficiently, and ensuring the security of our systems and information. Where we rely on legitimate interests, we will ensure that our interests are not overridden by your rights and freedoms.

Where we process **special category personal data**, including information concerning health, we will rely on an appropriate condition under Article 9 GDPR and the Data Protection Act 2018, including where processing is necessary for insurance purposes, fraud prevention, compliance with legal obligations, safeguarding vulnerable individuals, or the establishment, exercise or defence of legal claims.

Where we process **personal data relating to criminal convictions, offences, alleged offences or related security measures**, we will do so only where authorised by European Union or Irish law and subject to appropriate safeguards.

We may also process special category data and criminal offence data where necessary to establish, exercise or defend legal claims, investigate suspected fraud, or comply with our legal or regulatory obligations.

We use your personal information to:

- Investigate and assess claims and understand the circumstances of an incident.
- Verify information provided to us and assess the validity of claims.
- Prevent, detect and investigate fraud, financial crime and other unlawful activity.
- Communicate with you and with relevant representatives, advisers and third parties involved in a claim.
- Comply with legal, regulatory and professional obligations.
- Establish, exercise or defend legal rights and claims, including recovery actions.
- Maintain business, accounting and audit records.
- Improve our processes, systems, services and operational effectiveness.
- Provide training, quality assurance and security monitoring, including the recording or monitoring of calls where permitted by law.

3.4.5 What are the legal grounds on which we will use your personal information?

What is the purpose for using your personal information?	Legal grounds for using your personal information	Legal grounds for using your sensitive personal information
To handle a claim	• Legitimate Interests (to assess, investigate and manage claims and deal with them appropriately) • Compliance with a Legal Obligations	• Article 9(2)(f) GDPR – Processing necessary for the establishment, exercise or defence of legal claims
To comply with our legal or regulatory obligations including, for example, responding to personal data breaches or requests relating to your data protection rights.	• Legitimate Interests (to prevent fraud) • Compliance with a Legal Obligations	• Article 9(2)(g) GDPR – Processing necessary for reasons of substantial public interest • Article 9(2)(f) GDPR – Processing necessary for the establishment, exercise or defence of legal claims
To handle any complaints you may have and generally communicate with you.	• Compliance with a Legal Obligation • Legitimate Interests (to respond to communications, maintain compliance and manage regulatory requirements) • legitimate interest	• Article 9(2)(g) GDPR – Processing necessary for reasons of substantial public interest • Article 9(2)(f) GDPR – Processing necessary for the establishment, exercise or defence of legal claims
To pursue or defend legal claims and rights, including exercising our right of subrogation (that is to bring an action for recovery of the claim amount we have paid against you as the third party who we believe caused the loss or injury).	• Legitimate Interests (to pursue or defend legal claims or rights, including exercising our right of subrogation and recovering payment from the third party who caused the loss or injury) • Compliance with a Legal Obligation	• Article 9(2)(f) GDPR – Processing necessary for the establishment, exercise or defence of legal claims
To apply for and claim on our own insurance.	• Legitimate Interests (to maintain appropriate insurance arrangements and claim under those arrangements where necessary) • legitimate interest	• Article 9(2)(f) GDPR – Processing necessary for the establishment, exercise or defence of legal claims
For business purposes such as systems development, migration of systems, diagnosing any problems with our servers and website, improving the efficiency of our business, performing internal audits, analysing sales and usage of our services and products.	• Legitimate Interests (to run an efficient business and improve our business).	• Article 9(2)(g) GDPR – Processing necessary for reasons of substantial public interest (where Special Category Personal Data is processed)

3.4.6 Who will we share your personal information with?

We will only share your personal information where necessary for the purposes described in this notice, where we have a lawful basis under Article 6 GDPR and, where applicable, a condition under Article 9 GDPR or Article 10 GDPR. We do not sell your personal information.

We may share your personal information with:

- The policyholder, claimant and other insurers, reinsurers, brokers or intermediaries involved in the claim or recovery process.
- Claims handlers, loss adjusters, investigators, surveyors and other professional advisers engaged to investigate, assess or recover losses.
- Solicitors, barristers, courts, tribunals, mediators and other parties where necessary to establish, exercise or defend legal claims, including recovery proceedings.
- Witnesses and other persons connected with the incident where necessary for the investigation, defence or resolution of a claim or recovery action.
- Fraud prevention agencies, sanctions screening providers and organisations involved in the prevention, detection and investigation of fraud, money laundering or other criminal activity.
- Regulatory authorities, supervisory authorities and public bodies, including the Central Bank of Ireland, the Data Protection Commission, An Garda Síochána, the Revenue Commissioners, courts and other competent authorities where disclosure is required by law.
- Service providers acting on our behalf, including IT, cloud hosting, document management, audit and administrative support providers. Where they act as processors, they are subject to contracts meeting the requirements of Article 28 GDPR.
- Other companies within the Benefact Group where necessary for claims administration, recovery activities, fraud prevention, information security, internal audit, regulatory compliance or business continuity purposes.
- Our auditors, insurers and professional advisers.
- Prospective purchasers, merger partners or successor organisations in connection with a corporate transaction, subject to appropriate confidentiality obligations.

Where special category data or criminal offence data is disclosed, we will do so only where permitted by applicable EU or Irish law and subject to appropriate safeguards.

In some circumstances, we may act as a joint controller with another organisation. Where this occurs, we will comply with Article 26 GDPR and make the essence of the arrangement available on request.

Where personal data is transferred outside the European Economic Area (EEA), we will ensure appropriate safeguards are in place in accordance with Chapter V GDPR.

We will only share the minimum personal information necessary for the relevant purpose and will ensure recipients are subject to appropriate confidentiality and security obligations.

3.5 Witness to an incident

If you have witnessed an incident which has now become the subject of a claim, this section will be applicable to you and will provide key information about how we use your personal information.

3.5.1 What personal information will we collect?

- Your name and title, address, telephone numbers and email addresses, date of birth and gender.
- Your employment status and related information such as job title, employment history and education.
- Identity documents such as passport, driving licence and PPS number.
- Information which is available publicly such as via internet search engines and social media where we need to investigate potentially fraudulent claims.
- Any information which is related to the incident you witnessed.

3.5.2 What sensitive personal information will we collect?

- Information about your physical and mental health if you suffered an injury as a result of the incident you witnessed or where you disclose information to us, for example, referring to a disability you have.
- Information about any criminal offences you have been convicted for and any related information including about any offences or alleged offences you have committed or any court sentences which you are subject to. We process personal data relating to criminal convictions and offences only where authorised by applicable law and subject to appropriate safeguards designed to protect the rights and freedoms of individuals.

3.5.3 How will we collect your personal information?

Directly from you when we contact you to discuss the incident you witnessed.

We will also collect your personal information from:

- Those people involved in the incident such as the policyholder, the claimant and other witnesses.
- Other third parties involved in the incident from an insurance administration perspective such as brokers, insurers, claims handlers, loss adjusters and business partners.
- Third parties we have appointed to assist us in relation to the incident you witnessed such as medical experts, medical screening service providers and investigators.
- Other companies in the Benefact Group.
- Public sources such as court judgments, insolvency registers, internet search engines, social media.

3.5.4 What will we use your personal information for?

We use your personal information for a number of purposes relating to the investigation, assessment and handling of insurance claims. For each use of your personal information, we must identify a lawful basis under applicable data protection law.

When using your personal information, we may rely on one or more of the following legal bases:

- **Compliance with a legal obligation**, including obligations relating to fraud prevention, regulatory compliance, financial crime prevention, record keeping, responding to data protection requests, and communicating with regulatory or law enforcement authorities.
- **Our legitimate interests**, including investigating and managing claims, preventing fraud, exercising or defending legal rights, maintaining business records, improving our services, operating our business efficiently, and ensuring the security of our systems and information. Where we rely on legitimate interests, we will ensure that our interests are not overridden by your rights and freedoms.

Where we process **special category personal data**, including information concerning health, we will rely on an appropriate condition under Article 9 GDPR and the Data Protection Act 2018, including where processing is necessary for insurance purposes, fraud prevention, compliance with legal obligations, safeguarding vulnerable individuals, or the establishment, exercise or defence of legal claims.

Where we process **personal data relating to criminal convictions, offences, alleged offences or related security measures**, we will do so only where authorised by European Union or Irish law and subject to appropriate safeguards.

We may also process special category data and criminal offence data where necessary to establish, exercise or defend legal claims, investigate suspected fraud, or comply with our legal or regulatory obligations.

We use your personal information to:

- Investigate and assess claims and understand the circumstances of an incident.
- Verify information provided to us and assess the validity of claims.
- Prevent, detect and investigate fraud, financial crime and other unlawful activity.
- Communicate with you and with relevant representatives, advisers and third parties involved in a claim.
- Comply with legal, regulatory and professional obligations.
- Establish, exercise or defend legal rights and claims, including recovery actions.
- Maintain business, accounting and audit records.
- Improve our processes, systems, services and operational effectiveness.
- Provide training, quality assurance and security monitoring, including the recording or monitoring of calls where permitted by law.

3.5.5 What are the legal grounds on which we will use your personal information?

What is the purpose for using your personal information?	Legal grounds for using your personal information	Legal grounds for using your sensitive personal information
To investigate the claim made and to understand the incident which is the subject of the claim.	• Legitimate interest (to assess and investigate a claim and deal with it appropriately). • Compliance with a legal obligation.	• Article 9(2)(f) GDPR – Establishment, Exercise or Defence of Legal Claims. • Article 9(2)(g) GDPR – Substantial Public Interest.
To prevent any fraudulent claims.	• Legitimate interest (to prevent fraud). • Compliance with a legal obligation.	• Article 9(2)(f) GDPR – Establishment, Exercise or Defence of Legal Claims. • Article 9(2)(g) GDPR – Substantial Public Interest •
To comply with our legal or regulatory obligations including, for example, detecting unlawful acts or dishonesty, responding to personal data breaches or requests relating to your data protection rights.	• Compliance with a legal obligation. • Legitimate interest (to respond to all communications).	• Article 9(2)(f) GDPR – Establishment, Exercise or Defence of Legal Claims. • Article 9(2)(g) GDPR – Substantial Public Interest. •
For financial purposes such as maintaining management information and accounting records.	• Compliance with a legal obligation. • Legitimate interest (to maintain appropriate financial records)	• Article 9(2)(g) GDPR – Substantial Public Interest.
For business purposes such as systems development, migration of systems, diagnosing any problems with our servers and website, improving the efficiency of our business, performing internal audits, analysing sales and usage of our services and products.	• Legitimate interest (to run an efficient business and improve our business).	• Article 9(2)(g) GDPR – Substantial Public Interest (where processing is necessary for insurance administration purposes). • We do not generally use sensitive personal information for systems development activities unless strictly necessary and subject to appropriate safeguards.
To pursue or defend legal claims and rights, including exercising our right of subrogation (that is to bring an action for recovery of the claim amount we have paid against the third party who we believe caused the loss or injury).	• Legitimate interest (to pursue or defend legal claims or rights, including exercising our right of subrogation and recover payment from the third party who caused the loss or injury that you witnessed).	• Article 9(2)(f) GDPR – Establishment, Exercise or Defence of Legal Claims.

3.5.6 Who will we share your personal information with?

We will only share your personal information where necessary for the purposes described in this notice, where we have a lawful basis under Article 6 GDPR and, where applicable, a condition under Article 9 GDPR or Article 10 GDPR. We do not sell your personal information.

We may share your personal information with:

- The policyholder, claimant, defendant and other parties involved in the incident or claim where necessary to investigate, assess or resolve the claim.
- Insurers, reinsurers, brokers, claims handlers, loss adjusters, investigators, medical experts and other professional advisers involved in the management of the claim.
- Solicitors, barristers, courts, tribunals, mediators and other parties where necessary to establish, exercise or defend legal claims or rights.
- Fraud prevention agencies, sanctions screening providers and organisations involved in the prevention, detection and investigation of fraud, money laundering or other criminal activity.
- Regulatory authorities, supervisory authorities and public bodies, including the Central Bank of Ireland, the Data Protection Commission, An Garda Síochána, the Revenue Commissioners, courts and other competent authorities where disclosure is required by law.
- Service providers acting on our behalf, including IT, cloud hosting, document management, audit and administrative support providers. Where they act as processors, they are subject to contracts meeting the requirements of Article 28 GDPR.
- Other companies within the Benefact Group where necessary for claims administration, fraud prevention, information security, internal audit, regulatory compliance or business continuity purposes.
- Our auditors, insurers and professional advisers.
- Prospective purchasers, merger partners or successor organisations in connection with a corporate transaction, subject to appropriate confidentiality obligations.

Where special category data or criminal offence data is disclosed, we will do so only where permitted by applicable EU or Irish law and subject to appropriate safeguards.

In some circumstances, we may act as a joint controller with another organisation. Where this occurs, we will comply with Article 26 GDPR and make the essence of the arrangement available on request

Where personal data is transferred outside the European Economic Area (EEA), we will ensure appropriate safeguards are in place in accordance with Chapter V GDPR.

We will only share the minimum personal information necessary for the relevant purpose and will ensure recipients are subject to appropriate confidentiality and security obligations.

3.6 Brokers, Intermediaries and Other Business Partners

If you are a broker, intermediary, supplier, service provider, contractor, consultant or other business partner with whom we do business, this section explains how we collect, use and share your personal information.

3.6.1 What personal information will we collect?

We may collect and process the following categories of personal information about you:

- Your name, title, business address, telephone numbers and email addresses.
- Employment and professional information, including your job title, role, employer details, qualifications and professional experience.
- Identification and due diligence information where required, including copies of identification documents, regulatory registration details and information necessary to verify your identity.
- Bank account and payment details.
- Information obtained through sanctions screening, anti-money laundering checks, fraud prevention checks and other due diligence activities.
- Information obtained from publicly available sources, including company registers, professional

directories, regulatory registers, websites, internet searches and professional networking platforms such as LinkedIn.

- Records of communications and correspondence with you.
- Information relating to the services you provide to us, our customers or other business partners.

3.6.2 What Special Category Personal Data or Criminal Offence Data will we collect?

We do not generally collect Special Category Personal Data about business partners. However, in limited circumstances, we may process:

- Information relating to criminal convictions, offences, alleged offences or regulatory sanctions where this is necessary to conduct due diligence, comply with legal or regulatory obligations, prevent fraud, protect our business interests, or establish, exercise or defend legal claims.
- Limited Special Category Personal Data where it is provided to us in connection with a complaint, legal proceedings, fitness and probity assessment, regulatory investigation or other lawful business purpose.

3.6.3 How will we collect your personal information?

We collect personal information:

Directly from you:

- when you engage with us regarding the provision of services;
- during contract negotiations;
- through correspondence, meetings, telephone calls and emails; and
- when you provide documentation in support of due diligence or regulatory requirements.

We may also collect personal information from:

- your employer or organisation;
- insurance intermediaries, insurers, reinsurers and other insurance market participants;
- sanctions screening, fraud prevention and anti-money laundering service providers;
- credit reference agencies and financial crime prevention organisations;
- publicly available sources including the Companies Registration Office, regulatory registers, websites and professional directories;
- professional advisers and other business contacts; and
- other companies within the Benefact Group where there is a lawful basis to do so.

3.6.4 What will we use your personal information for?

We use your personal information for a number of business, legal and regulatory purposes.

When using your personal information, we may rely on one or more of the following legal bases:

- Performance of a contract, where processing is necessary to enter into, administer or perform a contract with you or your organisation.
- Compliance with a legal obligation, including compliance with anti-money laundering, sanctions, fraud prevention, taxation, accounting and regulatory requirements.
- Legitimate interests, including business administration, supplier management, procurement, governance, information security, risk management, fraud prevention, maintaining business records and improving our services.

Where we process Special Category Personal Data or criminal offence data, we will rely on one or more of the following legal bases:

- Processing is necessary for reasons of substantial public interest in accordance with Article 9(2)(g) GDPR and applicable Irish law.
- Processing is necessary for the establishment, exercise or defence of legal claims in accordance with Article 9(2)(f) GDPR.
- Processing is necessary to comply with legal and regulatory obligations.
- You have made the information manifestly public.
- You have provided your explicit consent, where consent is required.

3.6.5 What are the legal grounds on which we will use your personal information?

What is the purpose for using your personal information?	Legal grounds for using your personal information	Legal grounds for using your sensitive personal information
Conducting due diligence on brokers, suppliers and business partners.	- Compliance with a legal obligation; - Legitimate Interests	- Article 9(2)(g) GDPR (substantial public interest); - Article 9(2)(f) GDPR (legal claims).
Carrying out sanctions, anti-money laundering, fraud prevention and other financial crime checks.	- Compliance with a legal obligation; - Legitimate Interests	Article 9(2)(g) GDPR; Article 9(2)(f) GDPR.
Entering into, administering and managing contracts and business relationships.	- Performance of a contract; - Legitimate interests.	Article 9(2)(f) GDPR where required.
Communicating with you and managing the services you provide.	- Performance of a contract - Legitimate interests.	Article 9(2)(f) GDPR where required.
Responding to complaints, disputes, legal proceedings and regulatory enquiries.	- Compliance with a legal obligation; - Legitimate interests.	Article 9(2)(f) GDPR; Article 9(2)(g) GDPR.
Maintaining business records, accounting records, management information and audit records.	- Compliance with a legal obligation; - Legitimate Interests	Article 9(2)(g) GDPR where applicable.
Business improvement, systems development, information security, internal audit, risk management and business continuity planning.	Legitimate interests.	Article 9(2)(g) GDPR where applicable.

3.6.6 Who will we share your personal information with?

We may disclose your personal information to:

- Other companies within the Benefact Group.
- Insurance intermediaries, brokers, insurers, reinsurers and other insurance market participants where necessary for the administration of insurance business.
- Service providers, contractors and suppliers who support our business operations, including IT providers, cloud service providers, auditors, consultants and professional advisers.
- Solicitors, barristers, accountants, actuaries and other professional advisers.
- Organisations providing sanctions screening, anti-money laundering, fraud prevention, identity verification and financial crime monitoring services.
- The Central Bank of Ireland, the Data Protection Commission and other regulatory or supervisory authorities where disclosure is required or permitted by law.
- An Garda Síochána, the Revenue Commissioners, courts, tribunals and other public authorities where disclosure is required or permitted by law.
- Prospective purchasers, merger partners or successor organisations in connection with a corporate transaction, subject to appropriate confidentiality obligations.
- Our insurers, reinsurers and service providers appointed to assist with arranging, managing or administering our own insurance arrangements.

Where we share personal information with third parties, we take appropriate contractual, technical and organisational measures to ensure that it is protected and processed in accordance with applicable data protection laws.

3.8 Applications for Grants including bursaries

If you apply for a grant, bursary or other funding administered by Ecclesiastical, this section explains how we collect, use and share your personal information in connection with your application. This section applies to applicants, beneficiaries, referees and other individuals identified in support of an application.

3.8.1 What personal information will we collect?

The personal information we collect will depend on the nature of the grant or bursary programme and may include:

- *Your name, title, address, telephone number and email address.*
- *Information about the organisation you represent, where applicable.*
- *Information relating to your application, including details of the project, activity or purpose for which funding is sought.*
- *Information relating to your eligibility for a grant or bursary.*
- *Details of referees, sponsors or supporting individuals identified as part of the application process.*
- *Photographs, videos or other images provided as part of, or in support of, an application.*
- *Records of correspondence and communications with you.*
- *Bank account and payment information where funding is awarded.*
- *Information obtained from publicly available sources where relevant to assessing an application or verifying information provided to us.*

3.8.2 What Special Category Personal Data or Criminal Offence Data might we collect?

In limited circumstances, we may collect and process Special Category Personal Data where this is relevant to a grant or bursary application.

This may include:

- Information revealing religious or philosophical beliefs where the grant programme relates to faith-based organisations or activities.
- Information relating to health, disability or accessibility requirements where this is relevant to the application or participation in a funded activity.

- Other Special Category Personal Data where voluntarily provided by you and relevant to the assessment of your application.

We do not generally collect information relating to criminal convictions and offences for grant applications unless this is required for safeguarding, regulatory or legal reasons.

3.8.3 How will we collect your personal information?

We may collect personal information:

Directly from you:

- when you complete an application form;
- when you provide supporting documentation;
- when you communicate with us by email, telephone, post or online; and
- during the assessment and administration of your application.

We may also collect personal information from:

- referees or sponsoring organisations named in your application;
- organisations administering grant or bursary programmes on our behalf;
- publicly available sources used to verify information provided by applicants; and
- other companies within the Benefact Group where there is a lawful basis to do so.

3.8.4 What will we use your personal information for?

We use your personal information for a number of purposes connected with the administration of grants and bursaries.

When using your personal information, we may rely on one or more of the following legal bases:

- Legitimate interests, including assessing applications, administering grant programmes, preventing fraud and ensuring the fair and effective allocation of funding.
- Performance of a contract, where funding has been awarded and personal information is required to administer payments or fulfil programme requirements.
- Compliance with a legal obligation, including regulatory, financial reporting, audit, anti-fraud and record-keeping obligations.
- Consent, where consent is required for the publication of photographs, testimonials, case studies or promotional materials.

Where we process Special Category Personal Data, we will rely on one or more of the following legal bases:

- Article 9(2)(a) GDPR, where you have provided explicit consent.
- Article 9(2)(g) GDPR, where processing is necessary for reasons of substantial public interest and permitted by Irish law.
- Article 9(2)(e) GDPR, where the information has manifestly been made public by you.

3.8.5 What are the legal grounds on which we will use your personal information?

What is the purpose for using your personal information?	Legal grounds for using your personal information	Legal grounds for using your sensitive personal information
Assessing eligibility for a grant or bursary.	• Legitimate interests.	• Article 9(2)(g) GDPR where applicable.
Reviewing and evaluating applications.	• Legitimate interests.	• Article 9(2)(g) GDPR where applicable.
Verifying information provided by applicants.	• Legitimate interests • Compliance with a legal obligation.	• Article 9(2)(g) GDPR where applicable.
Administering successful applications and making payments.	• Performance of a contract; Legitimate interests.	• Article 9(2)(g) GDPR where applicable.
Preventing fraud and protecting grant funds.	• Compliance with a legal obligation • Legitimate interests.	• Article 9(2)(g) GDPR.
Maintaining records, governance and audit requirements.	• Compliance with a legal obligation • Legitimate interests.	• Article 9(2)(g) GDPR where applicable.
Publishing information about successful grants, including photographs, testimonials or case studies.	• Consent • Legitimate interests where appropriate.	• Article 9(2)(a) GDPR (Explicit Consent).

3.8.6 Who will we share your personal information with?

We may share your personal information with:

- Other companies within the Benefact Group.
- Organisations involved in assessing, administering or supporting grant and bursary programmes.
- Professional advisers, including auditors, legal advisers and consultants.
- Service providers acting on our behalf, including IT providers, cloud service providers, document management providers and payment service providers.
- Regulatory authorities, supervisory authorities and public bodies where disclosure is required or permitted by law.
- The Data Protection Commission, the Central Bank of Ireland, An Garda Síochána, the Revenue Commissioners, courts or other competent authorities where disclosure is required by law.
- Prospective purchasers, merger partners or successor organisations in connection with a corporate transaction, subject to appropriate confidentiality obligations.

Where grant recipients agree to participate in promotional, publicity or reporting activities, we may publish limited personal information, photographs, testimonials or case studies on our websites, social media channels, annual reports or other publications. We will obtain consent where required by applicable law.

Where personal information is shared with third parties, we take appropriate contractual, technical and organisational measures to ensure it is protected and processed in accordance with applicable data protection laws.

3.9 Users of our Websites and Digital Services

If you visit, access or use any Ecclesiastical website, portal, online service, mobile application or digital platform, this section explains how we collect, use and share your personal information.

Non-essential cookies and similar technologies are only used where you have provided consent where required by law. Consent may be withdrawn or amended at any time through our cookie preference management tool.

3.9.1 What personal information will we collect?

The personal information we collect will depend on the website, digital service or functionality you use, but may include:

- Your name, title, postal address, telephone number and email address where you choose to provide these details to us.
- Information submitted through online forms, enquiries, quote requests, event registrations, surveys or other website interactions.
- User account information, including usernames, passwords, security questions and authentication credentials where access to an online portal or restricted area is provided.
- Device and technical information, including IP address, browser type, operating system, device identifiers and website usage information.
- Information collected through cookies and similar technologies. Further information is available in our Cookie Policy.
- Marketing preferences and communication preferences.
- Records of correspondence and communications with us through websites, email, webchat or other digital channels.
- Information relating to your use of our websites and digital services, including pages viewed, resources accessed and interactions with website content.
- Information obtained from publicly available sources where relevant to responding to enquiries or providing services requested by you.

Please note that where you submit an insurance quote request, insurance application, claim notification or other insurance-related request through one of our websites, the relevant section of this Privacy Notice relating to that activity will also apply.

3.9.2 What Special Category Personal Data might we collect?

We do not generally seek to collect Special Category Personal Data through our websites.

However, we may receive Special Category Personal Data where:

- You provide such information within an enquiry, application, claim notification or communication submitted through our websites.
- Information relating to your religious or philosophical beliefs is provided in connection with faith-based insurance products, grant programmes or charitable activities.
- Information concerning health, disabilities or accessibility requirements is provided to facilitate your interaction with us or attendance at an event.

Where Special Category Personal Data is collected, we will only process it where we have identified an appropriate lawful basis under Article 9 GDPR and applicable Irish law.

3.9.3 How will we collect your personal information?

We collect personal information:

Directly from you:

- when you visit our websites;
- when you complete online forms;
- when you request information, quotations or services;
- when you subscribe to marketing communications;
- when you register for events, webinars or online services;

- when you participate in surveys or feedback activities; and
- when you communicate with us through digital channels.

We may also collect personal information through:

- cookies and similar technologies;
- analytics providers;
- advertising partners where permitted by law;
- social media platforms where you engage with our content;
- publicly available sources; and
- other companies within the Benefact Group where there is a lawful basis for sharing information.

3.9.4 What will we use your personal information for?

We use your personal information for a variety of purposes relating to the operation, management and improvement of our websites and digital services.

When using your personal information, we may rely on one or more of the following legal bases:

- Consent, where required by law, including for certain marketing activities and non-essential cookies.
- Performance of a contract, where necessary to provide a service or functionality requested by you.
- Compliance with a legal obligation, including responding to requests relating to your data protection rights and complying with regulatory requirements.
- Legitimate interests, including operating and improving our websites, maintaining security, preventing fraud, analysing website usage, responding to enquiries and communicating with users.

Where we process Special Category Personal Data, we may rely on:

- Article 9(2)(a) GDPR, where you have provided explicit consent.
- Article 9(2)(f) GDPR, where processing is necessary for the establishment, exercise or defence of legal claims.
- Article 9(2)(g) GDPR, where processing is necessary for reasons of substantial public interest under applicable law.
- Article 9(2)(e) GDPR, where the information has manifestly been made public by you.

3.9.5 What are the legal grounds on which we will use your personal information?

Purpose	Legal Basis for Personal Data	Legal Basis for Special Category Personal Data
Providing access to website content, online services and information requested by you.	• Performance of a Contract; Legitimate Interests.	• Article 9(2)(a) GDPR where applicable.
Responding to enquiries, complaints and other communications.	• Compliance with a Legal Obligation • Legitimate Interests.	• Article 9(2)(f) GDPR; • Article 9(2)(g) GDPR where applicable.
Managing user accounts and authentication processes.	• Performance of a Contract • Legitimate Interests.	• Article 9(2)(a) GDPR where applicable.
Monitoring, maintaining and improving website functionality, performance and security.	• Legitimate Interests.	• Article 9(2)(g) GDPR where applicable.
Detecting, preventing and investigating fraud, cyber threats and unauthorised access.	• Compliance with a Legal Obligation • Legitimate Interests.	• Article 9(2)(g) GDPR; • Article 9(2)(f) GDPR where applicable.
Analysing website usage, performance and user engagement.	• Legitimate Interests • Consent where required.	• Not normally applicable.
Sending marketing communications, newsletters and event invitations.	• Consent and/or • Legitimate Interests when permitted by applicable Irish ePrivacy legislation.	• Article 9(2)(a) GDPR (Explicit Consent).
Complying with legal, regulatory and governance requirements.	• Compliance with a Legal Obligation • Legitimate Interests.	• Article 9(2)(g) GDPR; Article 9(2)(f) GDPR where applicable.

3.9.6 Who will we share your personal information with?

We may share your personal information with:

- Other companies within the Benefact Group.
- Service providers who support the operation of our websites and digital services, including website hosting providers, cloud service providers, IT support providers, analytics providers, communication service providers and cybersecurity providers.
- Professional advisers including auditors, consultants and legal advisers.
- Marketing, event and communications service providers acting on our behalf.
- Social media and digital advertising platforms where you have consented to the use of relevant cookies or marketing technologies.
- The Central Bank of Ireland, the Data Protection Commission and other regulatory or supervisory authorities where disclosure is required or permitted by law.
- An Garda Síochána, the Revenue Commissioners, courts, tribunals and other public authorities where disclosure is required or permitted by law.
- Prospective purchasers, merger partners or successor organisations in connection with the sale, transfer or reorganisation of all or part of our business, subject to appropriate confidentiality obligations.

Where personal information is shared with third parties, we take appropriate contractual, technical and organisational measures to ensure that it is protected and processed in accordance with applicable data protection laws.

Where personal data is transferred outside the European Economic Area (EEA), we will ensure that appropriate safeguards are in place in accordance with Chapter V of the GDPR.

4. Targeted Advertising

We may use digital advertising platforms, social media platforms and online advertising networks, including LinkedIn, Google and Meta platforms, to promote our products, services, charitable activities, events and initiatives.

These activities may constitute direct marketing for the purposes of applicable data protection and electronic communications legislation.

Where permitted by law, we may use personal information that we hold about existing, former or prospective customers, policyholders, brokers, business partners, grant applicants or website users to help ensure that our advertising is relevant and appropriate.

This may include:

- displaying advertisements that are tailored to particular interests, sectors, professions or activities;
- promoting products or services that may be relevant to individuals who have interacted with us previously;
- measuring the effectiveness of advertising campaigns;
- understanding audience engagement with our advertisements; and
- identifying groups of individuals who may have similar characteristics or interests to our existing customers or supporters.

Where required by applicable law, we will obtain your consent before using cookies, advertising technologies or similar tracking technologies for targeted advertising purposes.

Where you have consented to marketing and advertising cookies, we may use information collected through our websites and digital services to:

- personalise advertising content;
- display advertisements on third-party websites and platforms;
- analyse advertising effectiveness; and
- improve the relevance of future advertising campaigns.

In certain circumstances, we may use audience matching or "lookalike audience" services provided by third-party advertising platforms. For example, we may securely provide limited personal information, such as an email address, to a social media or advertising platform so that it can identify individuals who share similar characteristics with existing customers or supporters and display our advertisements to those individuals.

Where audience matching or similar advertising services are used:

- we will only do so where there is an appropriate lawful basis;
- we will ensure that appropriate data sharing and processing arrangements are in place;
- we will only share the minimum amount of personal information necessary for the purpose; and
- we will comply with applicable GDPR and ePrivacy requirements.

Where information is shared with digital advertising providers, those providers may act as independent controllers of the personal information they receive. Information about how those providers process personal information can be found in their respective privacy notices.

The legal basis upon which we rely for targeted advertising activities will depend on the circumstances and may include:

- your consent, particularly where cookies or similar technologies are used;
- our legitimate interests in promoting our products, services and charitable activities, where permitted by applicable Irish ePrivacy legislation and where such interests are not overridden by your rights and freedoms.

You have the right to object at any time to the processing of your personal information for direct marketing purposes, including profiling related to direct marketing.

You may exercise this right by:

- clicking the unsubscribe link included in marketing communications;

- amending your cookie preferences through our website;
- adjusting your advertising preferences on relevant social media or advertising platforms; or
- contacting us using the details set out in Section 10.

Electronic marketing communications, including email and SMS communications, will only be sent where permitted by applicable data protection and ePrivacy legislation and, where required, with your consent.

Where you object to direct marketing, we will stop processing your personal information for those purposes unless we are otherwise permitted or required to do so by law.

If personal information is transferred outside the European Economic Area (EEA) as part of advertising or marketing activities, we will ensure that appropriate safeguards are implemented in accordance with Chapter V of the GDPR.

5. Automated Decision-Making, Profiling & Artificial Intelligence (AI)

Ecclesiastical may use automated processes, profiling techniques and artificial intelligence ("AI") technologies in connection with the provision of insurance products and services, the administration of policies, claims handling, fraud prevention, customer service, risk management and the operation of our business.

5.1 Automated Decision-Making

In certain circumstances, we may make decisions about you using automated means. This means that a decision is made by technological means without direct human involvement at the point the decision is taken.

For example, we may use automated systems and underwriting rules to:

- assess eligibility for insurance cover;
- determine whether a proposed risk falls within our underwriting criteria;
- calculate insurance premiums;
- identify potentially fraudulent or unusual transactions;
- assess claims information; and
- support operational and administrative decision-making processes.

Where an automated decision produces legal effects concerning you, or similarly significantly affects you, we will ensure that appropriate safeguards are in place in accordance with Article 22 of the GDPR.

These safeguards may include:

- obtaining human intervention;
- enabling you to express your point of view;
- allowing you to contest the decision; and
- reviewing the decision where appropriate.

Where automated decision-making is used in underwriting, pricing, fraud detection or claims assessment, we will provide additional information concerning the significance and likely consequences of the processing where required by law.

If you wish to obtain further information regarding any automated decision affecting you, please contact us using the details set out in Section 10 of this Privacy Notice.

5.2 Profiling

We may use profiling techniques to better understand our customers, policyholders, claimants, website users and business partners.

Profiling involves analysing information about you to evaluate particular characteristics, preferences or behaviours.

We may use profiling:

- to assess insurance risk;
- to identify products and services that may be relevant to you;
- to improve customer service and communications;
- to identify customers who may require additional support;

- to monitor and improve business performance;
- to detect and prevent fraud, financial crime and other unlawful activity; and
- to support claims assessment and underwriting decision-making.

Profiling does not necessarily result in an automated decision and may be used simply to assist our employees in reaching decisions.

Where profiling is used, we will take steps to ensure that it is fair, proportionate and compliant with applicable data protection legislation.

5.3 Artificial Intelligence and Machine Learning

We use artificial intelligence ("AI") and machine learning ("ML") technologies to support the delivery of our services and to improve the efficiency, accuracy and effectiveness of our business operations.

AI and ML technologies may be used for purposes including:

- supporting underwriting assessments and risk evaluation;
- assisting with claims handling and claims triage;
- identifying potential indicators of fraud or financial crime;
- analysing documents, correspondence and communications;
- generating summaries of claims, customer interactions or technical information;
- improving operational efficiency and service delivery;
- monitoring and improving the quality of our processes, products and services;
- identifying trends and patterns within our business operations;
- enhancing information security and cyber security controls; and
- maintaining and improving data quality and accuracy.

AI-generated outputs are not relied upon in isolation where human review is necessary or appropriate. Decisions affecting individuals may be reviewed by appropriately trained personnel to ensure fairness, accuracy and compliance with legal and regulatory requirements.

5.4 Lawful Basis

Where we process personal information using automated decision-making, profiling or AI technologies, we do so on the basis of one or more of the following lawful bases:

- the performance of a contract;
- compliance with a legal obligation;
- our legitimate interests in operating and improving our business, products and services; or
- your consent, where consent is required by law.

Where Special Category Personal Data is processed in connection with automated decision-making, profiling or AI technologies, we will rely on an appropriate condition under Article 9 GDPR and applicable Irish data protection legislation.

5.5 Your Rights

You have rights in relation to automated decision-making, profiling and AI processing.

Subject to applicable law, these rights may include:

- the right to obtain meaningful information about the logic involved in automated decision-making;
- the right to request human review of certain automated decisions;
- the right to express your point of view;
- the right to challenge a decision;
- the right to object to certain types of profiling or processing carried out on the basis of legitimate interests; and
- the right to lodge a complaint with the Data Protection Commission.

If you wish to exercise any of these rights, please contact us using the details set out in Section 10 of this Privacy Notice.

6. How long do we keep personal information for?

We will retain your personal information only for as long as is necessary to fulfil the purposes for which it was collected, including satisfying legal, regulatory, accounting, tax, audit, reporting and business requirements.

The period for which we retain personal information depends on a range of factors, including:

- the nature of our relationship with you;
- the type of product, service or activity involved;
- the purpose for which the information was collected;
- applicable legal and regulatory requirements;
- relevant limitation periods for legal claims;
- our obligations to maintain business records;
- regulatory guidance and industry standards; and
- our legitimate business needs.

As a regulated insurance undertaking, we are required to maintain certain records for extended periods in order to:

- administer insurance policies and claims;
- comply with regulatory obligations;
- investigate and prevent fraud and financial crime;
- establish, exercise or defend legal claims;
- respond to complaints and disputes;
- comply with tax, accounting and audit requirements; and
- maintain appropriate governance, risk management and business continuity arrangements.

Where personal information is no longer required, we will securely delete, destroy, anonymise or otherwise dispose of it in accordance with our records management and data retention policies.

6.1 Insurance Policies and Claims

Retention periods for insurance records vary according to the nature of the policy and the associated risk.

For example:

- policy documentation, underwriting records and customer correspondence may be retained for a number of years after a policy has ended;
- claims files may be retained for extended periods following settlement, depending on the nature of the claim and applicable legal limitation periods;
- records relating to long-tail liability risks may be retained for significantly longer periods where claims may arise many years after the policy period has ended;
- fraud prevention and financial crime records may be retained for periods necessary to meet legal, regulatory and operational requirements.

In certain circumstances, liability claims may emerge many years after an insured event has occurred. Where necessary and proportionate, policy and claims information may therefore be retained for extended periods to protect the interests of policyholders, claimants and Ecclesiastical.

6.2 Marketing Information

Where we process personal information for marketing purposes, we will retain that information until:

- you withdraw your consent (where consent is relied upon);
- you object to the processing;
- you unsubscribe from receiving marketing communications; or
- we determine that the information is no longer required for the relevant marketing activity.

We may retain limited information relating to your marketing preferences to ensure that your preferences are respected in the future.

6.3 Website and Digital Service Information

Information collected through our websites and digital services will be retained for periods that are appropriate to the purpose for which it was collected, including:

- maintaining website security;

- analysing website performance and usage;
- investigating suspected fraud or cyber security incidents;
- complying with legal obligations; and
- maintaining records of communications and enquiries.

Further information regarding the retention of cookies and similar technologies can be found in our Cookie Policy.

6.4 Legal and Regulatory Requirements

In some circumstances, we may be required to retain personal information for longer periods in order to:

- comply with applicable laws and regulatory requirements;
- respond to requests from regulators or public authorities;
- establish, exercise or defend legal claims;
- resolve complaints, disputes or investigations;
- comply with court orders; or
- protect the rights, property and interests of Ecclesiastical, our customers and other stakeholders.

6.5 Further Information

If you would like further information regarding the retention of your personal information, including the retention period that applies to a particular category of information, please contact us using the details set out in Section 10 of this Privacy Notice.

We will be happy to provide additional information regarding our records retention practices and the safeguards we apply to protect personal information throughout its lifecycle.

Detailed retention periods are maintained within our Records Retention Schedule and are reviewed regularly to ensure compliance with legal, regulatory and operational requirements.

7. What is our approach to sending your personal information overseas

In the course of providing our products and services, administering insurance policies, handling claims, managing our business operations and working with service providers, it may be necessary for us to transfer personal information to countries outside the European Economic Area ("EEA") and, where relevant, the United Kingdom.

The EEA comprises the member states of the European Union together with Iceland, Liechtenstein and Norway.

Some of the organisations with whom we share personal information, including members of the Benefact Group, service providers, technology providers, professional advisers, claims service providers, fraud prevention providers and other business partners, may be located outside the EEA or may process personal information outside the EEA.

Where we transfer personal information outside the EEA, we will ensure that an appropriate level of protection is provided in accordance with Chapter V of the General Data Protection Regulation ("GDPR").

7.1 How We Protect Personal Information Transferred Outside the EEA

Where personal information is transferred to a country that has not been recognised by the European Commission as providing an adequate level of protection, we will implement appropriate safeguards, which may include:

- entering into Standard Contractual Clauses ("SCCs") approved by the European Commission;
- implementing additional technical, organisational and contractual safeguards where required;
- relying on Binding Corporate Rules where applicable;
- relying on approved codes of conduct or certification mechanisms where available; or
- using another lawful transfer mechanism permitted under Chapter V GDPR.

Where personal information is transferred to a jurisdiction that has been recognised by the European Commission as providing an adequate level of protection, the transfer may take place on the basis of that adequacy decision.

7.2 Circumstances Where Transfers May Occur

International transfers may occur where necessary for:

- the administration of insurance policies;
- underwriting and risk assessment activities;
- claims handling and claims investigations;
- fraud prevention and financial crime monitoring;
- obtaining professional advice;
- business continuity and disaster recovery arrangements;
- information technology, cloud hosting and support services;
- customer service and communications;
- regulatory reporting and compliance activities; and
- the operation and management of our business.

Where appropriate, personal information may be transferred to service providers, reinsurers, legal advisers, loss adjusters, claims handlers, technology providers and other organisations that support the provision of our services.

7.3 Transfers Necessary for Insurance and Claims Purposes

In certain circumstances, international transfers may be necessary to provide insurance services or administer claims.

For example:

- where a claim involves an incident that occurred outside the EEA;
- where a policyholder requires assistance while travelling abroad;
- where specialist claims, legal, medical or technical expertise is required in another jurisdiction; or
- where an overseas insurer, reinsurer, service provider or professional adviser is involved in the administration of a policy or claim.

Where such transfers occur, we will ensure that an appropriate legal basis and transfer mechanism applies unless a specific derogation under Article 49 GDPR permits the transfer.

7.4 Countries to Which Personal Information May Be Transferred

Personal information may be transferred to, or accessed from, countries including:

- the United States of America;
- India;
- Israel;
- the Philippines; and
- other countries in which our service providers, technology partners, reinsurers, claims service providers, professional advisers or business partners operate.

The countries to which personal information is transferred may change from time to time as our business operations and service provider arrangements evolve.

7.5 Your Rights and Further Information

You may request further information regarding the safeguards we apply when transferring personal information outside the EEA, including details of the relevant transfer mechanism relied upon.

If you would like further information about our international transfers of personal information, please contact us using the details set out in Section 10 of this Privacy Notice.

8. How do we protect your information?

We are committed to protecting the confidentiality, integrity, availability and security of the personal information entrusted to us.

We maintain appropriate technical and organisational measures designed to protect personal information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure, unauthorised access or any other form of unlawful processing.

These measures are reviewed regularly to ensure that they remain appropriate, taking into account the nature of the personal information processed, the risks involved, technological developments and applicable legal and regulatory requirements.

8.1 Information Security Framework

We operate a comprehensive information security and data protection framework designed to safeguard personal information throughout its lifecycle.

This framework includes:

- documented information security, privacy and data protection policies and procedures;
- governance arrangements that oversee information security and data protection risks;
- information classification and handling requirements;
- risk assessment and risk management processes;
- incident management and breach response procedures; and
- regular monitoring and review of security controls and practices.

8.2 Access Controls

We restrict access to personal information to individuals who have a legitimate business need to access it.

Access controls may include:

- role-based access permissions;
- user authentication controls;
- password management standards;
- multi-factor authentication where appropriate;
- monitoring of user activity; and
- periodic review of access rights.

All employees, contractors and service providers with access to personal information are subject to confidentiality obligations and are required to process personal information in accordance with applicable laws and internal policies.

8.3 Technical Security Measures

We implement a range of technical safeguards designed to protect personal information, including:

- encryption technologies for data at rest and in transit where appropriate;
- firewalls and network security controls;
- anti-malware and endpoint protection solutions;
- vulnerability management and patching processes;
- secure system development and change management procedures;
- logging and monitoring capabilities; and
- backup and recovery arrangements designed to support operational resilience.

8.4 Supplier and Third-Party Management

Where we engage third-party service providers to process personal information on our behalf, we take reasonable steps to ensure that they maintain appropriate security and confidentiality standards.

This may include:

- conducting due diligence before engagement;
- entering into data processing agreements where required under Article 28 GDPR;
- assessing information security controls and certifications;
- monitoring supplier performance; and
- requiring providers to implement appropriate technical and organisational measures.

8.5 Staff Training and Awareness

We provide employees with appropriate information security and data protection training and awareness programmes.

This helps ensure that personal information is handled appropriately and that employees understand their responsibilities regarding privacy, confidentiality and information security.

8.6 Testing and Continuous Improvement

We regularly evaluate and improve our information security arrangements through activities such as:

- internal reviews and audits;
- risk assessments;
- security testing and monitoring;

- incident analysis and lessons learned reviews;
- regulatory compliance assessments; and
- ongoing review of policies, procedures and controls.

8.7 Reporting Security Concerns

Although we apply appropriate security measures, no method of transmission over the internet or method of electronic storage can be guaranteed to be completely secure.

If you believe that your interaction with us is no longer secure, or if you become aware of any actual or suspected security issue involving your personal information, please contact us immediately using the details provided in Section 10 of this Privacy Notice.

9. Your rights

Under the General Data Protection Regulation ("GDPR") and the Data Protection Act 2018, you have a number of rights in relation to the personal information we hold about you.

These rights are not absolute and may be subject to certain conditions, limitations or exemptions under applicable law. Where we are unable to comply with a request, we will explain the reasons and inform you of any rights available to you.

In certain circumstances, exercising your rights may impact our ability to provide insurance products or services, administer a policy, investigate or settle a claim, comply with legal obligations or maintain our business relationship with you.

9.1 Right of Access

You have the right to request confirmation as to whether we process your personal information and, where we do, to obtain a copy of that information together with certain information about how it is used.

This is commonly referred to as a Data Subject Access Request.

Where possible, we will provide the information in electronic form if the request is made electronically, unless you request otherwise.

9.2 Right to Rectification

You have the right to request that inaccurate personal information is corrected and that incomplete personal information is completed.

We encourage you to notify us as soon as possible if any of the information we hold about you changes or becomes inaccurate.

Where appropriate, we will also notify third parties to whom we have disclosed the information.

9.3 Right to Erasure

You have the right to request the deletion of your personal information in certain circumstances, including where:

- the information is no longer necessary for the purpose for which it was collected;
- you withdraw consent where consent is the legal basis for processing;
- you successfully object to the processing;
- the information has been unlawfully processed; or
- deletion is required to comply with a legal obligation.

This right is not absolute and may not apply where we are required to retain information for legal, regulatory, insurance, accounting, fraud prevention, audit or claims handling purposes.

9.4 Right to Restriction of Processing

You have the right to request that we restrict the processing of your personal information in certain circumstances, including where:

- you contest the accuracy of the information;
- the processing is unlawful, but you do not want the information erased;
- we no longer require the information, but you require it for legal claims; or
- you have objected to processing pending consideration of that objection.

9.5 Right to Data Portability

Where processing is carried out by automated means and based on your consent or the performance of a contract, you may have the right to receive the personal information you have provided to us in a structured, commonly used and machine-readable format.

You may also have the right to request that the information be transmitted directly to another organisation where technically feasible.

9.6 Right to Object

You have the right to object to the processing of your personal information where we rely on legitimate interests as our legal basis.

Where you exercise this right, we will stop processing your personal information unless we can demonstrate compelling legitimate grounds which override your interests, rights and freedoms, or where processing is required for the establishment, exercise or defence of legal claims.

9.7 Right to Object to Direct Marketing

You have the absolute right to object at any time to the use of your personal information for direct marketing purposes.

This includes profiling to the extent that it relates to direct marketing.

If you object to direct marketing, we will stop processing your personal information for those purposes.

You can exercise this right by:

- using the unsubscribe facility provided in marketing communications;
- updating your communication preferences where available; or
- contacting us using the details provided in Section 10.

9.8 Right to Withdraw Consent

Where we rely on your consent to process personal information, you have the right to withdraw that consent at any time.

Withdrawal of consent will not affect the lawfulness of any processing carried out before consent was withdrawn.

Please note that where consent is necessary for the provision of a particular product, service or activity, withdrawal of consent may affect our ability to continue providing that product, service or activity.

9.9 Rights Relating to Automated Decision-Making

You have rights in relation to certain forms of automated decision-making and profiling.

Where a decision is based solely on automated processing and produces legal effects concerning you, or similarly significantly affects you, you may have the right to:

- obtain human intervention;
- express your point of view;
- request a review of the decision; and
- challenge the outcome of the decision.

Further information about our use of automated decision-making, profiling and artificial intelligence is set out in Section 5.

9.10 Exercising Your Rights

If you wish to exercise any of your data protection rights, please contact us using the details provided in Section 10.

We may ask you to provide proof of identity before responding to your request in order to protect your personal information and ensure that it is disclosed only to the correct individual.

We will respond to your request in accordance with applicable data protection legislation.

9.11 Right to Lodge a Complaint

If you have concerns about the way we process your personal information, we encourage you to contact us first so that we have the opportunity to investigate and address your concerns.

You also have the right to lodge a complaint with the Data Protection Commission.

Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28
Ireland

Telephone: +353 (0)57 868 4800

Website: www.dataprotection.ie

Lodging a complaint with the Data Protection Commission does not affect any other legal rights or remedies available to you.

You also have the right to seek a judicial remedy where you consider that your rights under data protection law have been infringed.

10. Contacting us

If you have any questions about this Privacy Notice, wish to exercise any of your data protection rights, would like further information about how we process your personal information, or wish to make a complaint regarding the handling of your personal information, please contact us using the details below.

Data Protection Officer

Ecclesiastical Insurance Office plc
4th Floor, The Heysham,
73 North Wall Quay, Dublin,
D01 V2F4
Ireland

Telephone: +353 (0)1 619 0300

Email: ComplianceIreland@ecclesiastical.com

Alternatively, you may contact our Group Data Protection Office at:

Email: dataprotection@benefactgroup.com

Exercising Your Rights

If you wish to exercise any of your rights under the GDPR, including:

- the right of access;
- the right to rectification;
- the right to erasure;
- the right to restriction of processing;
- the right to data portability;
- the right to object;
- the right to withdraw consent; or
- rights relating to automated decision-making,

please contact us using the details set out above.

To protect your personal information, we may request information to verify your identity before responding to your request.

Complaints

We are committed to resolving concerns regarding the processing of personal information fairly and promptly.

If you have a concern about the way we process your personal information, we encourage you to contact us first so that we have the opportunity to investigate and resolve the matter.

If you are not satisfied with our response, you may lodge a complaint with the Data Protection Commission.

Data Protection Commission

Data Protection Commission
21 Fitzwilliam Square South
Dublin 2
D02 RD28

Ireland

Telephone: +353 (0)57 868 4800

Website: www.dataprotection.ie

Further Information

If you require further information about:

- the categories of personal information we process;
- the lawful bases we rely upon;
- international transfers of personal information;
- retention periods;
- data protection rights; or
- any aspect of this Privacy Notice,

please contact us using the details above and we will be happy to assist.

11. Updates to this notice

We keep this Privacy Notice under regular review to ensure that it remains accurate, up to date and reflective of our legal, regulatory and operational requirements.

From time to time, we may update this Privacy Notice to reflect:

- changes in applicable laws or regulations;
- guidance issued by regulatory or supervisory authorities;
- developments in data protection practices;
- changes to our products, services or business activities;
- the introduction of new technologies or processing activities; or improvements to the way we collect, use, share or protect personal information.

Where appropriate, we will notify affected individuals of material changes to this Privacy Notice through appropriate communication channels, including our website, policy documentation, customer communications or other means as required by law.

The most current version of this Privacy Notice will always be available on our website.

We encourage you to review this Privacy Notice periodically to remain informed about how we collect, use and protect your personal information.

Last reviewed and updated:	12 October 2026
-----------------------------------	------------------------