UNUM EEA Group
Information for policyholders of group schemes

Unum is an employee benefits provider. The policyholder is the employer who has chosen one of Unum's insurance policies.

We set up and administer group schemes and provide policy documents to evidence the contract in place between us and the policyholder.

As a regulated insurer, we do not complete third party assessments or due diligence type questionnaires, including those focusing on information security, data protection and business continuity, and will not sign separate or side agreements with our policyholders. The nature of the product and service we provide has led to a well-established and robust compliance programme that we can monitor and evidence to our regulators' satisfaction.

Our approach is consistent with other insurance providers and relates back to guidance given by the Chartered Institute of Procurement and Supply (CIPS) on Group Risk Insurance policies. It identifies the high degree of protection in the UK insurance sector and references the importance of being regulated by the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA).

We do acknowledge however that policyholders have a duty of care to their employees. We are happy to provide a number of documents for assurance, which are accessible via links in the summary section of this document.

Our approach is also the result of the following reasons:

- We are a Data Controller in this relationship (not a Data Processor), as reaffirmed by GDPR legislation, and comply directly with all laws and regulations. We process policyholders' data to set up and administer the policy, and decide what information we need from the policyholder to insure them. We do not process data for policyholders in a typical data processing supplier contract.
- We are an FCA and PRA regulated business, and are registered with the Information Commissioner's Office (ICO). We embody these regulatory requirements in a number of detailed internal policies and procedures. We have robust plans and processes in place for data protection, information security, business continuity, etc. These also comply with a rigorous set of rules, including treating customers fairly, systems and controls, financial management and corporate governance, to name just a few.
- We have our own Code of Conduct that applies to all staff. All of our employees must undergo background checks, training and certification confirming they have read and understood their obligations under the code.
- We work with a network of data processors appointed once thorough due diligence and appropriate contractual wording has been put in place. These data processors would never be deemed as a sub-processor/vendor acting on your behalf.
- Voluntary flexible benefits, such as Dental Cover, are products specifically selected by the employee, who provides us with the necessary information to enable us, as the Data Controller, to set up and administer the insurance contract. Please note that while flexible benefit plans such as Unum Dental are general insurance plans, these are still set up with employers and made available to employees, so are subject to the same controls as other Unum products.

In summary

Unum does not:

- Complete individual questionnaires or separate agreements for policyholders (including those specific to GDPR) where we are the sole Data Controller for insurance purposes.
- Agree to supplier/vendor codes of conduct. It is not practical, nor appropriate, for us to agree to thousands of customers' individual codes of conduct. The differences between codes would prove impossible to implement and monitor, and their provisions could contradict our obligations under FCA and PRA regulation. This stance is also supported by **CIPS guidance**.
- Allow audits or share commercially sensitive documentation, including internal policies and control frameworks, with external parties such as policyholders.

Unum do:

- Have company policies in place which are reviewed regularly and implemented across the business. This includes a **programme** to ensure we are GDPR compliant.
- Have public initiatives and statements available on unum.co.uk - please view these **here**.
- Have a Data Privacy and Information Security pack, which provides **an overview** of the safeguards in place and outlines our commitment to maintaining external security accreditations that can be shared with customers, including Cyber Essentials and KPMG validated SOC 2 report.

Associated documents and links

- GDPR and Unum EEA Group
- GDPR FAQs
- Data Privacy and Information Security
- Privacy Notice
- CIPS

Unum Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority. Registered Office and mailing address: Milton Court, Dorking, Surrey RH4 3LZ. Registered in England 983768. Unum Limited is a member of the Unum Group of Companies.