

GDPR FAQs

Does Unum act as a Data Controller or Data Processor?

Unum UK Group of Companies provides employee benefit insurance products. We are registered for such purposes with the Information Commissioner's Office as a Data Controller.

Will you be in a position to meet your obligations under the GDPR by 25th May 2018?

Yes – we have been running a project since early 2017 involving all business areas to ensure we will be compliant for 25th May 2018.

What are you doing to ensure GDPR compliance?

Our project has:

- Established a governance structure for oversight of GDPR compliance efforts
- Put in place a core team to provide guidance, share regulatory updates and set priorities
- Created a multi-disciplinary working group to identify and address gaps and to drive compliance across the business
- Introduced a Data Protection Charter and suite of covering policies
- Implemented software to manage our data retention policies
- Reviewed policies, procedures and contracts to ensure compliance with GDPR provisions
- Engaged with external experts, including obtaining independent legal advice, to assist with overall compliance programme
- Managed a comprehensive project plan and communication plan.

Will you be able to demonstrate compliance with the GDPR?

Yes – we have developed a Data Asset Register to record all business activities, the lawful basis for managing personal data and how this is stored.

How does Unum collect personal data?

We receive data in a variety of ways, including from customers and suppliers. This information is only collected for legitimate purposes which are integral to the running of our business.

Do you keep records of which lawful processing conditions apply to your processing activities?

The lawful basis for processing was identified during the data mapping phase of the GDPR programme. The lawful basis is also supported by various measures which include our Statutory Notices and consent notices, and data retention and disposal routines. We also conduct periodic reviews of business processes to assure compliance with this approach.

How are you approaching the revised information GDPR requires to be provided to customers?

We have updated all procedures and processes to include the additional requirements introduced by GDPR, including:

- Updating our existing Statutory (Privacy) Notices and consent clauses for customers
- Review and update of our existing processes to manage breaches and complaints
- Review and update of our Data Subject Access Request (DSAR) process

Do you have processes in place for your record-keeping activities – eg. breach reporting, processing activities, updating records?

Yes – compliance is monitored through our Data Protection team, Risk, Compliance function and Internal Audit function.

Have your staff be provided with training on compliance with the GDPR?

Yes – all staff have been provided with GDPR awareness training and our annual Data Protection and Information Security training programme has been updated to reflect the GDPR.

Do you notify clients immediately if you become aware of a data breach?

Yes – our breach process has been reviewed to ensure that any notifiable breaches are actioned as soon as possible, and in any event, within the 72 hours of us being made aware of the breach.

Do you have technical and organisational measures in place to protect personal data from accidental or unlawful destruction, loss alteration, unauthorised disclosure or access?

Yes – we have strict controls over all our personal data use and these are continually reviewed to ensure that these provide the highest possible standards of protection.

Do you have a policy on conducting Data Privacy Impact Assessments (DPIA)?

Yes – we have undertaken DPIA's on all business areas as part of our GDPR programme and have an agreed policy in place to be followed for any new business initiatives impacting data protection.

How will Unum ensure business partners are GDPR compliant?

We are undergoing a thorough exercise updating all relevant contracts with third parties to reflect GDPR requirements. This will ensure that any such processing of personal data takes place under appropriate contractual terms and proportionate to the business need.

What is Unum's approach to record retention and data disposal?

We control our use of personal information according to our Data Retention Policy which stipulates the period for which all data is retained and subsequently disposed of, for both the structured and unstructured systems and applications. There are also technology updates being introduced which support adherence to this policy.

How does Unum control the transfer of data outside of the EEA?

We ensure that any data required to be transferred outside of the EEA is referenced in appropriate Data Transfer Agreements which use Model Clauses approved by the European Commission.

Has Unum appointed a Data Protection Officer (DPO)?

Yes – we have a designated DPO who can be contacted at:

DPO, Unum Limited,
Milton Court,
Dorking, Surrey,
RH4 3LZ.

Telephone 01306 887766.

unum.co.uk

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. We monitor telephone conversations and e-mail communications from time to time for the purposes of training and in the interests of continually improving the quality of service we provide.