UK GDPR
Protecting personal data

The implementation of the General Data Protection Regulation (GDPR) on 25 May 2018 created many questions with respect to Group Protection insurance. However, in reality, few changes were needed to the way our customers share data with us. To help explain this, we've answered some common questions employers have asked us.

What is GDPR?

The General Data Protection Regulation (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission have strengthened and unified data protection for all individuals within the European Union. As an EU member on 25 May 2018, the UK incorporated the new regulations into UK law.

Following the UK's withdrawal from the European Union, GDPR was transposed into UK law.

References to GDPR within this leaflet should be read as the data protection laws and regulations that apply within the UK (currently the Data Protection Act 2018), and any changes to EU legislation and regulation that have legal effect in the UK.

What is the Data Protection Act 2018?

The Data Protection Act 2018 applies to UK organisations. It modernised and extended UK data protection laws, and helped clarify how GDPR is applied within the UK.

The Data Protection Act 2018 includes paragraphs relating to insurance. These paragraphs allow us to receive and use employee data provided by employers for Group Protection insurance, without us obtaining consent from each employee.

It's important for employees to know we hold some of their personal information for a Group Protection policy, and that they have data rights. As we have no direct means of contacting the employees, we're asking employers to share our Privacy Policy with the employees they insure.

Do you have a Privacy Policy?

Yes, our Privacy Policy explains what we do with the information we collect and is available at: https://www.legalandgeneral.com/privacy-policy/

We've posted it online to help make sure our customers always have easy access to the latest version. We ask employers to share this Privacy Policy with the people they ask us to insure under our Group Protection policies.

Do you have a separate data protection agreement, or something in your contract terms?

No, we don't believe there is a need for separate agreements relating to protecting data.

We're a UK-regulated financial services company, a registered Data Controller, and solely responsible for the personal information we hold relating to Group Protection insurance. We have clear legal and regulatory responsibilities, and GDPR didn't our status as a Data Controller. Our regulator requires us to provide a policy document which records everything to do with the insurance cover, and there was no need for new GDPR content.

Product literature and forms

Some of our processes collect medical and health information, for example, to process medical underwriting requests and claims for group income protection or critical illness cover. Our forms seek to collect a person's:

- explicit consent to process their medical and health information, and
- separate consent to access medical reports, if needed.

The forms also provide access to the Privacy Policy.

Legal & General

Please use the latest versions of our forms to avoid delays and inconvenience.

We regularly review and update all our literature, replacing the old versions at the same web address (URL). You may wish to save a link to forms you frequently use instead of a local copy.

Please see our current literature and forms held under our document library.

Are you a Data Controller or Data Processor?

With Group Protection contracts of insurance, the employer or firm are customers of the insurer. As the insurer, we operate independently as a data controller, and our customer has no liability for the data we hold.

Us being the data controller is based on the principles that:

- We need the data to assess the insurance risk and administer the insurance contract.
- We're processing the data for our own purpose, and not for the customer.
- The insurance policy is a product solely developed and provided by us, that the customer has purchased.
- It isn't something that's been jointly developed with the customer, and the customer has no say in how we use the data.

We have registered with the Information Commissioner's Office (ICO) as a data controller. You can check our **ICO registration**.

Do I need a Data Processing agreement with you?

No, you don't. We do not process data on behalf of our customers.

As we're the data controller, we don't believe there is any need for an agreement regarding data protection or data processing and this is not something we can enter into.

Why do you need employee data?

We need data to assess the insurance risk and run the Group Protection policies we provide. As the insurer and sole data controller we decide the information we need from our commercial customers. We limit the information we ask for to the minimum amount that's needed to run the policy.

When would you seek individual consent from members?

Some of our processes require employees to provide medical and health information, for example, to process medical underwriting, or claims for Group Income Protection or Critical Illness Cover.

Our forms provide access to our Privacy Policy, explain how we use the information, and who we may share it with. We seek the employees' explicit consent to use their medical and health information in this way.

Our forms will include a separate section if we need to seek medical reports from the employee's doctor, or any other health professional they may have seen. This will explain the employee's rights relating to medical reports, and seek their consent for the reports to be sent to us.

The information we gather for these processes is provided directly to us from the individual, their doctor or a treating specialist/therapist, and any independent medical examiners.

Do I need individual consent from my employees to send you their information?

You will need to send us personal information about your employees who are, or become, eligible for cover. You'll also need to give further details about your employees if you claim. This may include medical and health information. You need to satisfy yourself of a legal basis that allows you to send us these details, or consider seeking appropriate consent (explicit consent in the case of medical or health information).

With a focus on Group Income Protection claims, our leaflet about **sharing the personal data of absent employees** explores different legal basis for sharing an employee's personal details.

How long do you hold information?

Different policy activities use different types of information, with each having its own data retention procedure. As a Data Controller we only keep information for as long as we need it. This could be for many years to allow for the long-term nature of our policies, claims, legal and regulatory needs.

How do you keep information secure?

We have robust governance policies that cover many topics including Information Protection, IT Security and Data Retention. We meet the UK regulatory standards on protecting the information provided by our customers. Processes for Data Retention, Breaches and Subject Access Requests are familiar to us as an insurer who has acted as a Data Controller for many years.

Who do you share information with?

We'll disclose when necessary, personal information to other companies within the Legal & General group of companies, your financial adviser, our professional advisers, reinsurers, regulatory bodies, government, law enforcement and fraud prevention agencies, future owners of our business, and the third-party suppliers, contractors and service providers we engage to help us provide our services to you.

If you make a claim, we will share information, where necessary, with other insurance companies to prevent fraudulent claims.

If we share personal information, it will be in line with our **privacy policy**. Please share this policy with your employees so they understand what we do with the information we collect.

Do you share information outside of the UK and European Economic Area (EEA)?

As our policies provide you with an indefinite contract, we are unable to predict how our services will change over time. We may need to transfer your information to countries outside the UK and European Economic Area to provide these services. This may include sharing information with suppliers, some of whom may be multinational companies. We'll take all reasonable steps to make sure the data is treated securely and in accordance with our privacy policy. We'll only transfer the data to a recipient outside the UK and EEA where we're permitted to do so by law.

What happens if my employees want Legal & General to delete their personal information?

The personal information we ask for is limited to the minimum amount we need to provide the insurance cover and pay claims. It helps us set premium levels and terms for cover, administer the policy, complete

medical underwriting and validate claims. We cannot operate the contract without this information, and GDPR permits us to keep it while we have a contractual need.

If an employee asks us to delete their personal information, we will still have a contractual need to keep it to help us provide the policy cover. The contractual need continues after the group policy ends, and we will need to keep the personal information for a limited period. This help us answer your questions, process claims that you may submit late. We may also keep the personal data for as long as we have a legal or regulatory need to do so.

While we cannot delete the personal information straight away, we have governance in place to make sure personal data is only kept for as long as we need it.

Do you store personal data as defined within GDPR and what protections do you have to safeguard personal data?

Legal & General stores a large amount of personal information in order to conduct our business with our policyholders and investors and other people we have relationships with. We hold personal data in accordance with data protection law and maintain technical and organisational measures to ensure the security of the personal data including, measures against unauthorised or unlawful processing and accidental loss or destruction of personal data.

These measures include utilising firewalls, virus protection, dual-factor authentication, imposing removable media restrictions, web-browser controls, adopting email and information classification policies, data centre restrictions and surveillance, risk assessments and penetration testing.

We have policies covering information handling and confidentially, access management, data retention, intrusion security controls and other appropriate information protection and usage set by the Chief Information Security Officer and Data Protection Officer. Data is processed in accordance with those policies and group policies are subject to at least an annual review.

We hold data in repositories which are subject to controls as determined by the Chief Information Security Officer and documented in formal IT Security and Data Protection policies. We do not provide detailed specifications in order to protect the data and ensure our security is not compromised by making the security configuration or security information public.

Data may be stored in many formats, for example paper filing, paper archives, server-based internal networks, third-party applications, cloud-based systems. Our governance policies cover all these formats.

Can you provide information about your IT Security?

We're the sole data controller of the data we hold and the customer has no liability in respect of it. We are not processing data on behalf of our customers. Given that customers have no liability for the data we hold, there shouldn't be any need to complete IT Security questionnaires and it is our policy that we don't complete these.

However, high-level information about our IT Security can be made available if you sign a confidentiality agreement. Please sign and return this **confidentiality agreement** if you would like us to share this information with you.

What if I have further questions in respect of data security or UK GDPR?

Please get in touch with your usual Group Protection contact or visit the Information Commissioner's Office and their **Guide to the UK General Data Protection Regulation (UK GDPR)**.

Contact us

0345 026 0094
We may record and monitor calls. Call charges will vary.

group.protection@landg.com

Group Protection
Legal & General Assurance Society Limited
Knox Court
10 Fitzalan Place
Cardiff
CF24 0TL

Q0056838 08/22

Legal & General