

# GDPR Update – February 2018

---

The forthcoming implementation of the General Data Protection Regulation (GDPR) on 25 May 2018 is creating many questions with respect to Group Protection insurance. We are working through the regulations to make sure we are ready when they take effect. However, in reality, we don't expect many changes will be required to the way our customers share data with us. To help explain this, we have answered some common questions that employers may have with respect to their Group Protection policies.

## 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 intend to strengthen and unify data protection for all individuals within the European Union. As the UK will still be a member of the EU on 25 May 2018, the regulations must be incorporated into UK law.

## What is changing as a result of GDPR?

As a UK-regulated financial services company registered as a Data Controller, our legal and regulatory responsibilities are clear. So far we haven't needed to add anything to our Group Protection policy documents about protecting personal data. Our regulator requires us to document everything to do with the insurance cover within the policy document; there is no need for a separate agreement.

We have a group-wide project for GDPR which is reviewing all our affected governance policies, processes, the consent, disclosure and privacy notices we give. Currently we cannot say if these might change.

## What is the Data Protection Bill?

The bill for the legislation to implement the GDPR in the UK was published on 13 September 2017. Within the bill, there is a clause that allows us to receive employee data from employers to provide Group Protection insurance. This can be done without us obtaining consent from each employee. The bill is still being debated in parliament so is subject to change, but we expect Group Protection insurers will still be able to receive employee data in a very similar way to as they do now.

**We will provide a further update when the bill becomes law.**

## Are you a Data Controller or Data Processor?

With Group Protection contracts of insurance, the employer or firm are customers of the insurer. Often customers incorrectly assume that we're processing data on their behalf (as a data processor). In fact, we're the sole data controller for all the data that we hold and therefore the customer has no liability in respect of it.

Us being the data controller is based on the principle 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 sole data controller. Our role won't change when the GDPR become law in May 2018. You can check our [ICO registration](#).

### Do I need a Data Processing agreement with you?

No, you don't.

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. The information we ask for is essential to provide the insurance. We are processing the data for our own purpose and not on behalf of our customers.

### Do you seek individual consent from members?

If we need specific medical information, for example to confirm and process a claim or to medically underwrite, we have processes in place to:

- request the individual's consent in relation to data that we gather from them; and
- explain their rights to access the information we hold on them.

The information we gather is provided directly to us from the individual, their doctor and treating specialists/therapists, and any independent medical examiner we may appoint.

### 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 secure information?

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.

### Do you share information outside of the 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 European Economic Area to provide these services. This may include sharing information with suppliers, some of whom may be multinational companies. Our procurement processes help make sure the suppliers we engage protect our customer information through contract, audit and due diligence.

### Can you provide information about your IT Security?

As stated previously, we're the sole data controller for 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 release Security information.

### What if I have further questions in respect of data security?

Please get in touch with your usual Group Protection contact.

## Contact us



**0345 072 0751**

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