# Direct Line Insurance Services Business to Business Statement on General Data Protection Regulation ("GDPR") Compliance

## GENERAL INFORMATION

| | |
|---|---|
| **Name of organisation** | Direct Line Insurance Services ("DLIS") |
| **DLIS address** | Churchill Court, Westmoreland Road, Bromley, Kent BR1 1DP |
| **Web address** | https://www.directlinegroup.co.uk/ |
| **ICO Registration** | The ICO registration number for DLIS is Z5715071.<br><br>The ICO registration number for U K Insurance Limited, which underwrites and administers insurance policies as a Data Controller, is Z6487866. |
| **DPO Contact details** | Chris Whitewood, Data Protection Officer<br>Tel: 01651 832493<br>E: Christopher.Whitewood@directlinegroup.co.uk |

## GDPR ADHERENCE

| | |
|---|---|
| **GDPR adherence – general** | DLIS has undertaken an extensive programme to provide for compliance with all aspects of GDPR. |
| **Documented policies** | Our internal 'Minimum Standards' ("MS") form part of our Insurance Policy Framework and reflect the requirements of GDPR.<br><br>These MSs are applicable and available to all employees. |
| **Operating Model** | We have an appointed Data Protection Officer and a dedicated Privacy and Information Management team. |
| **Ongoing monitoring** | Adherence to data protection legislation, including GDPR, is continuously monitored by DLIS, including through:<br>• Monthly MI and reporting<br>• Assurance activity undertaken by the Privacy & Information Management team and our internal audit function.<br>• Quality Assurance as part of BAU activity<br>• Supplier reviews |

## PERSONAL DATA COLLECTED AND PURPOSES FOR WHICH IT IS USED

We always aim to collect only such personal data that is adequate, relevant and limited to what is necessary, in relation to the purposes for which they are processed, in line with Article 5(c) of the GDPR.

**Information we may collect about you**

Depending on the arrangement between the parties, we may collect, retain and share information such as:

- Contact Information (name. email address, phone number)
- Correspondence information (e.g. email correspondence, meeting notes, telephone calls)
- Corporate financial information (invoices that may contain your information).
- Information relating to criminal convictions, for example in order to undertake required due diligence.

We aim to collect only such personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

**Purposes for which your personal data may be used**

We may collect, use and share your personal information in order to facilitate business partnerships with your organisation. This may include to:

- Pursue or fulfil a contract, agreement or partnership with your organisation.
- Explore future partnership opportunities with your organisation.
- Comply with the law regarding data sharing.
- Comply with our contractual obligations.

## LEGAL BASIS FOR PROCESSING

The information you provide to us is required to facilitate business partnerships and is provided by you on a voluntary basis. We may rely on the following legal bases of processing:

**Necessary to perform a contract**

To allow DLIS to enter into a contract with you or your organisation.

**Legitimate interests**

For example, to allow DLIS to provide you or your organisation with information about new commercial opportunities.

**Legal obligations**

To allow DLIS to fulfil our legal and regulatory obligations.

**Consent**

Consent is only relied on where no other legal basis applies.

## STORAGE LIMITATION

**Retention of Personal Data**

We maintain a comprehensive retention schedule for the retention of Personal Data. As a general rule, where we are collecting your Personal Data in connection with a corporate project, we will retain your information for 6 years from the end of the financial year in which that project closes unless we continue to have a relationship with you. There may be exceptions where we need to retain your information for longer, for example if we are required to retain your information for any legal reasons.

Where there are technical reasons why Personal Data cannot be deleted, we put this data 'beyond use', in line with ICO guidance.

**Destruction of media**

We have a documented approach to the destruction of media (e.g. IT hardware, laptops, CDs, USBs).

## DATA SUBJECT RIGHTS

Under Data Protection law, you have various rights in relation to your own data (i.e. where you are the 'data subject'), which are summarised below:

| | |
|---|---|
| **Right of Access** | You have the right to request a copy of all the personal information that we have about you. Please note that you can directly access the data we hold about you by visiting our email alert page. |
| **Right to Rectification** | You have the right to ask us to update information that we hold about you where it is incorrect or incomplete. Please note that you can change your alerting preferences or unsubscribe at any time directly by visiting our email alert page. |
| **Right to Erasure** | You have the right to request the deletion of your personal data, for example where processing is no longer necessary for the purposes for which the data were collected. |
| **Right to Restriction of Processing** | You can ask us to stop processing your data (i.e. we cannot make any further changes, delete, or share it). For example, this could be where you wish to challenge the accuracy of data or where you make use of your 'Right to Object'. |
| **Right to Data Portability** | You are entitled to an electronic copy of the data that you provided to us as part of subscribing to the email alert service. |
| **Right to Object** | You can object to processing conducted under the 'Legitimate Interest' condition and we must then cease processing unless we can demonstrate compelling grounds. |
| **Right to withdraw consent** | You have the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. |
| **Automated decision-making and profiling** | You have the right not to be subject to a decision which is based solely on automated processing (including profiling), which would have a significant or legal effect on you. You have the right to contact us to express your point of view and challenge the decision. |

DLIS has an established process to identify, escalate and manage all Data Subject Rights requests. A dedicated and trained team is in place to co-ordinate responses to Data Subjects in line with GDPR requirements, including responding within the required 1month timeframe.

Specific queries in relation to exercising your Rights should be directed to DLIS's Data Protection Officer, whose details are shown at the beginning of this document.

## INFORMATION ASSET REGISTERS

| | |
|---|---|
| **Information Asset Registers ("IAR")** | DLIS maintain an IAR in line with GDPR requirements in Article 30. |

## PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

| | |
|---|---|
| **Data Privacy Impact Assessments** | DPIAs are mandatory as part of any change process. All DPIAs are reviewed by a Privacy professional and centrally logged. |

## OTHER THIRD PARTIES

| | |
|---|---|
| **Third party contracts** | Contracts with processors and sub-processors reflect GDPR requirements. |
| **Third party assurance** | DLIS have a third party assurance review process which periodically assesses third parties' information security and privacy controls and supporting processes, taking into account the requirements of regulators (including the ICO) and DLIS's internal requirements. |

## DATA PROTECTION INCIDENTS

| | |
|---|---|
| **Personal data incidents** | Our personal data incident management meets GDPR requirements, is documented, has been communicated to all staff through mandatory training modules and is available on the intranet to all members of staff.<br><br>All incidents are investigated, logged and appropriate mitigating actions taken to prevent recurrence, including a review of policies and procedures. The risk of harm and distress to data subjects is assessed |
| **Notification of breaches to the ICO** | Processes and procedures have been put in place to identify if a breach has occurred; assess the incident and risk to data subjects. This includes engagement of DPO to consider referral to ICO. DLIS's internal Risk Framework requires all breaches to be reported in line with GDPR requirements. |

## INTERNATIONAL TRANSFERS

| | |
|---|---|
| **DLIS location** | DLIS is UK based. |
| **Data transfers outside of the EEA** | The security of data being transferred outside of the EEA is a key consideration of Data Protection Impact Assessments. DLIS has processes in place to ensure that any and all transfers of its Personal Data outside the EEA are subject to adequate levels of protection for Data Subjects. |

## CONFIDENTIALITY, TRAINING AND PHYSICAL SECURITY

| | |
|---|---|
| **Confidentiality** | Confidentiality clauses are included as standard in all employee and supplier contracts.<br><br>User Access controls are in place to ensure access to systems is restricted to those members of staff who need access for their roles. Processes are in place to validate user access periodically. |
| **Training and awareness** | Data Protection, Information Security and Information Management training is mandatory for all employees. This is reviewed and refreshed on an annual basis. Ad-hoc training is delivered where training needs are identified. |
| **Physical Security** | DLIS requires that all sites have access controls to mitigate unauthorised access. The controls deployed include a combination of man guarding, proximity reader automated access, car park barriers/gates and shutters etc. |

## COMPLAINTS

If you have any concerns about the way in which we are using your personal information, please direct them to DLIS's Data Protection Officer in the first instance, whose details are shown at the beginning of this document.

You also have the right to complain about how we treat your personal information to the Information Commissioner's Office ("**ICO**"). The ICO can be contacted at:

ICO website: http://ico.org.uk/global/contact-us

ICO telephone: 0303 123 1113

ICO textphone: 01625 545860