Data Privacy Policy

Summary

Direct Line Group (DLG) has implemented a control framework to manage privacy and security risks to meet our responsibilities under data protection legislation, following regulatory and industry guidance and standards. Governance forums ensure privacy and security considerations receive high levels of visibility. All business areas within the Group are required to meet the standards set out in our privacy and security framework. Our internal standards require all business lines and subsidiaries to adhere to and evidence compliance with UK GDPR obligations, including implementing privacy by design, fulfilling data subject rights and reporting and resolving potential incidents. Security controls have been reviewed against UK GDPR requirements. All staff, including temporary staff and contractors, are trained on their data protection and security responsibilities and are contractually subject to confidentiality obligations.

Direct Line Group's Privacy Programme

The Group has implemented a clear Target Operating Model to instill a privacy focused culture across the organisation, through a Three Lines of Defence Model. We have an established first line Privacy team who work with business areas to build privacy requirements into our processes. Regular assurance and audit activity is conducted to demonstrate our commitment to our privacy standards.

Our Privacy and Data Protection Officer (DPO) provides independent oversight and challenge as part of our second line risk function in accordance with their responsibilities under UK GDPR and provides Board Level reporting at least annually. This is supported by regular reporting to the Board by the Chief Information Security Officer on security aspects.

Internal Audit, who perform robust periodic audits to assess compliance, constitute our third line of defence. Identified control deficiencies are logged, tracked and managed to resolution.

Privacy Framework

DLG maintains an extensive privacy and security framework to meet the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018, including processes to enable DLG to demonstrate accountability and adherence to UK GDPR obligations. Records of processing activities have been documented. All business areas are required to collect and process personal information fairly and lawfully, including clearly defining the purpose of any use of data, as outlined within our Privacy Policy.

Controls are in place to ensure that personal information collected is accurate and up to date.

Our fair processing notices (Privacy Policy) provide transparency to individuals as to how their personal information will be processed. These notices meet the requirements of UK GDPR to ensure individuals are informed as to what personal information is collected, how it will be processed, why we are legally permitted to use their data in that way and how to exercise their rights. For further information, please see:

- Our customer Privacy Notice which relates to the provision of insurance services and is presented to all customers and potential customers. You can see this here: https://u-k-insurance.co.uk/brands-policy.html

- Our Corporate Website Privacy Notice which relates to personal data collected through this corporate website. You can see this here: https://www.directlinegroup.co.uk/en/site-services/corporate-website-privacy-notice.html

An Employee Privacy Notice is also provided internally to all DLG staff.

Processes to fulfil requests from individuals exercising their rights under UK GDPR are embedded within DLG, allowing individuals to receive responses within the prescribed timelines under UK GDPR. Individuals are clearly informed how to exercise all of their rights under GDPR in our Customer Privacy Notice and Corporate Website Privacy Notice to facilitate a response from our dedicated Data Rights Team. Where possible, functionality has been created to allow individuals to correct their information easily and self-serve where possible.

Concerns, complaints and queries about our use of personal information can be addressed directly to the organisation's Data Protection Officer, contact information is available in our Privacy Notices.

We have a bespoke privacy incident reporting process which has been enhanced to enable all incidents, breaches and near misses to be identified and escalated to the Privacy Team and DPO for review. This process enables DLG to assess any risk of harm to data subjects and meet requirements to notify the Information Commissioner's Office ('ICO') within 72 hours as prescribed under GDPR. This process also enables data subjects to be notified as soon as possible, where required.

Our change governance process enables early assessment of privacy and security risks and a culture of Privacy and Security by Design. All new initiatives which involve the use of personal information are required to undertake an impact assessment, through use of an online

tool, which are reviewed by security and privacy teams for validation before the initiative can go live. We ensure all systems which are used to record or process personal information have the functionality to correct, delete and, where appropriate, support a request to exercise the right to erasure (right to be forgotten) and restrict processing of personal information. We also apply the UK GDPR concept of 'data minimisation', collecting the minimum amount of personal information necessary to fulfil our purposes for processing the information, using technology solutions to support this. DLG also use technology to anonymise or pseudonymise data sets where required.

Significant investment has been made to our retention strategy so that personal information is not kept longer than required, and the defined periods have been set out within our retention schedule. Once the retention period ends, the data is either deleted, anonymised or put beyond use in accordance with the ICO guidance. As a general rule, customer information is retained for 6 years from the end of the customer's relationship with DLG to comply with regulatory requirements or to allow us to process claims. Data related to unaccepted quotes are retained for 90 days or for the period the quote is valid for plus 30 days (whichever is the greater), and then for a limited time after for fraud prevention purposes.

Requests for information from government bodies, law enforcement agencies and public authorities are handled by a dedicated disclosure unit who follow regulatory guidelines on data sharing practices and in compliance with data protection legislation.

Direct Line Group's Security Programme

The DLG Information Security, Risk and Assurance department is led by the Chief Information Security Officer (CISO), who has responsibility for cyber security, risk and business resilience programs. The CISO reports to the Chief Operating Officer (COO). Periodic updates on cyber security, technology risk and business resilience programmes are provided to the Board of Directors and executive management.

Appropriate technical and organisational measures are implemented to protect personal information. DLG utilises sophisticated tools designed to protect information and prevent data breaches. In addition, we proactively perform self-assessments against our regulatory frameworks such as the NIST cyber security Framework and compliance with our internal cyber security controls is validated through the use of security monitoring utilities and through rigorous audits. External independent audits are conducted at a minimum of once every two years. Legal, regulatory and contractual obligations are reflected in and exceeded by the mandatory requirements of DLG's Minimum Standards framework, against which performance is measured and audited.

DLG's encryption policy is to secure data in accordance with industry best practice, such as compliance with encryption requirements set out in the PCI DSS both at rest and in transit. We participate in vulnerability information sharing networks and track industry and government intelligence sources for impact in the marketplace and deploy necessary updates as appropriate. DLG has a robust software patch management process that includes risk assessment and risk-based update schedules. These systems are designed, implemented and maintained to provide a high level of security to safeguard sensitive data.

DLG has implemented a Cyber Response Framework. The framework is a set of coordinated procedures and tasks that are executed to ensure timely and accurate resolution of computer security incidents.

Governance

The Policy and Minimum Standards Framework governs our business directorates and helps to ensure that personal and company data is protected in line with our obligations under data protection legislation and ensure adequate technical and organisational measures are in place to protect personal information. All business areas are required to comply with the Minimum Standards and attest and evidence compliance with each standard.

We have an established Privacy & Data Protection Minimum Standard..

DLG also has a Cyber Risk Minimum Standard, which incorporates a number of Information Security Minimum Requirements (ISMRs) including user access controls to limit access to personal information to a need to know basis, network, application and operational security and third party supplier security. All ISMRs are reviewed on an annual basis.

The Information Management Minimum Standard defines our approach to record keeping and retention of both personal and corporate information.

Privacy and data security is within the remit of our Risk Management Committee, who review our Policy and Minimum Standard Framework on an annual basis. We have also established a group-wide Privacy & Information Management Steering Committee which reviews any privacy risks and developments across the business. Issues are escalated to the Customer Conduct Committee, Operational Risk Committee, Risk Management Committee or Board Risk Committee as appropriate.

Third Parties

DLG shares the minimum data necessary with third parties and specifically notes how data is shared in the Privacy Notice and Privacy Policy. The organisation utilises a comprehensive information security due diligence and oversight process for its third-party vendors. Prior to the commencement of services, we perform a risk/impact rating assessment of all vendors that will have access to and process DLG information and conduct formal, comprehensive privacy and security assessments on service providers. Re-assessment occurs on an ongoing basis, the frequency of which is determined based on a risk assessment and rating process. The assessment process utilises a variety of tools to address aspects of the vendors' cyber security controls and policies, including business resilience and privacy and data protection. Regular onsite assessments are undertaken for vendors perceived to carry higher inherent risk.

All third parties are expected to meet data protection standards including UK GDPR obligations. UK GDPR compliant contractual clauses are in place with third parties to ensure they meet the high standards demanded. We also require all suppliers to meet our high security standards and adhere to our Information Security Minimum Requirements. Suppliers are contractually required to meet and demonstrate adherence to these requirements.