GDPR Compliance Statement

Introduction

The *General Data Protection Regulation ("GDPR")* came into force across the European Union on 25th May 2018 and brought with it the most significant changes to data protection law in two decades. Based on privacy by design and taking a risk-based approach, GDPR has been designed to meet the requirements of the digital age.

The Regulation aimed to standardise data protection laws and processing across the EU; affording individuals stronger, more consistent rights to access and control their personal information.

The Commitment

Riley Lifting Equipment is committed to ensuring the security and protection of the personal information that it controls and / or processes, and to provide a compliant and consistent approach to data protection. Riley Lifting Equipment has always had a robust and effective data protection program in place which complied with existing laws and abided by the principles of data protection. However, Riley Lifting Equipment recognises its obligations in updating and expanding this program to meet the demands of GDPR and the Data Protection Act 2018.

Riley Lifting Equipment is dedicated to safeguarding the personal information for which it is responsible and in developing a data protection regime that is effective, fit for purpose and demonstrates an understanding of, and appreciation for GDPR and the Data Protection Act 2018. The preparation and objectives for GDPR compliance have been summarised in this statement which includes the development and implementation of new data protection roles, policies, procedures, controls and measures to ensure maximum ongoing compliance.

How GDPR is being Implemented

Riley Lifting Equipment already has a consistent level of data protection and security across its organisation: it strives to be fully compliant with the GDPR. To achieve this, it has implemented the following:

- ***Information Audit*** - carrying out a company-wide information audit to identify and assess what personal information is held, where it comes from, how and why it is processed, and to whom it is disclosed if at all.
- ***Policies & Procedures*** - Revising data protection policies and procedures to meet the requirements and standards of GDPR and all relevant data protection laws, including:
    - ***Data Protection*** - the main policy and procedure document for data protection has been overhauled to meet the standards and requirements of GDPR. Accountability and governance measures are in place to ensure that the staff at Riley Lifting Equipment understand, adequately disseminate and evidence their obligations and responsibilities with a dedicated focus on privacy by design and the rights of individuals.

- ***Data Retention & Erasure*** - the retention policy and schedule have been updated to ensure that the *'data minimisation'* and *'storage limitation'* principles are met, and that personal information is stored, archived and destroyed compliantly and ethically. Dedicated erasure procedures have been put in place to meet the new *'Right to Erasure'* obligation and members of staff are aware of when and how this and other data subjects' rights apply, along with any exemptions, response timeframes and notification responsibilities.

- ***Data Breaches*** - the breach procedures ensure that there are safeguards and measures in place to identify, assess, investigate and report any personal data breach at the earliest possible time. These procedures are robust and have been disseminated to all relevant employees, making them aware of the reporting lines and steps to follow.

- ***International Data Transfers & Third-Party Disclosures*** - where Riley Lifting Equipment stores or transfers personal information outside the EU, there are robust procedures and safeguarding measures in place to secure, encrypt and maintain the integrity of data. These procedures include a continual review of the countries with sufficient data protection laws, as well as provisions for binding corporate rules; standard data protection clauses or approved codes of conduct for those countries without sufficient data protection laws. Strict due diligence checks are carried out with all recipients of personal data to assess and verify that they have appropriate safeguards in place to protect the information, ensure enforceable data subject rights and have effective legal remedies for data subjects where applicable.

- ***Data Subject Access Request*** - procedures have been revised to accommodate the 30-day timeframe for providing the requested information and for making this provision free of charge. The new procedures detail how to verify the data subject, what steps to take for processing an access request, what exemptions apply and a suite of response templates to ensure that communications with data subjects are compliant, consistent and adequate.

- ***Legal Basis for Processing*** - processing activities are being reviewed to identify the legal basis for processing and ensuring that each basis is appropriate for the activity it relates to. Where applicable, records of processing activities are maintained, ensuring that the obligations under Article 30 of the GDPR and Schedule 1 of the Data Protection Act 2018 are met.

- ***Data Privacy Notice*** - the Data Privacy Notice is being revised to comply with GDPR, ensuring that all individuals whose personal information is processed have been informed of why that information is needed, how it is used, what the individuals' rights are, which parties the information is disclosed to and what safeguarding measures are in place to protect their information.

- ***Obtaining Consent*** - the consent mechanisms are being revised for obtaining personal data, ensuring that individuals understand what they are providing, why and how it is used and giving clear, defined ways to consent to their information being processed. Stringent processes for recording consent have been developed, making sure that an affirmative opt-in can be evidenced, along with time and date records, with an easy to see and access way to withdraw consent at any time.

- ***Direct Marketing*** - the wording and processes for direct marketing are being revised, including clear opt-in mechanisms for marketing subscriptions; a clear notice and method for opting out and providing unsubscribe features on all subsequent marketing materials.

- ***Data Protection Impact Assessments (DPIA)*** – where personal information that is considered high risk is processed, involving large scale processing or includes special category / criminal

conviction data, stringent procedures and assessment templates for carrying out impact assessments have been developed that comply fully with the GDPR's Article 35 requirements. Documentation processes that record each assessment have been implemented to rate the risk posed by the processing activity and implement mitigating measures to reduce the risk posed to the data subject(s).

- ***Processor Agreements*** –if any third-party is used to process personal information (*e.g. payroll, recruitment, hosting, etc.*), there are compliant processor agreements and due diligence procedures for ensuring that they meet and understand their GDPR obligations. These measures include initial and ongoing reviews of the service provided, the necessity of the processing activity, the technical and organisational measures in place and the ongoing compliance with GDPR.

- ***Special Categories Data -*** where any special category information is obtained and processed, it is done in complete compliance with the Article 9 requirements and high-level encryptions and protections is used on all such data. Special category data is only processed where necessary and is only processed where the appropriate Article 9(2) basis or the Data Protection Act Schedule 1 condition have first been identified. Where consent for processing is relied upon, this is explicit and is verified by a signature, with the rights to modify or remove consent being clear.

Data Subject Rights

In addition to the policies and procedures mentioned above that ensure individuals can enforce their data protection rights, there is easy to access information about an individual's right to access any personal information that is held about them including:

- Exactly what personal data is held about them;
- The purposes of the processing;
- The categories of personal data concerned;
- The recipient(s) to whom the personal data has / will be disclosed;
- How long their personal data is intended to be stored for;
- If the data was not collected directly from them, information about the source;
- The right to have incomplete or inaccurate data about them corrected or completed and the process for requesting this;
- The right to request erasure of personal data (*where applicable*) or to restrict processing in accordance with data protection laws, as well as to object to any direct marketing activity and to be informed about any automated decision-making that is used;
- The right to lodge a complaint or seek judicial remedy and who to contact in such instances.

Information Security & Technical and Organisational Measures

Riley Lifting Equipment takes the privacy and security of individuals and their personal information very seriously and takes every reasonable measure and precaution to protect and secure the personal data that is processed. There are robust information security policies and procedures in place to protect personal information from unauthorised access, alteration, disclosure or destruction: there are several layers of security measures used to achieve this.

GDPR Roles and Employees

Riley Lifting Equipment has a designated Data Protection Officer (or senior individual responsible for compliance with Data Protection legislation). Riley Lifting Equipment is committed to developing and implementing its roadmap for complying with GDPR on an ongoing basis. This individual is responsible for promoting awareness of GDPR across the organisation, identifying any problem areas and implementing the appropriate policies, procedures and measures.

Riley Lifting Equipment understands that continuous employee awareness and understanding is vital to the continued compliance of GDPR and has involved its employees in preparation plans. It has implemented an employee training program which will be provided to all appropriate employees, and forms part of the induction and ongoing training program.

If you have any questions about Riley Lifting Equipment's compliance with GDPR, please get in touch!