Document Reference	Status	
GR-GDPR-DPP	Approved	GUY-RAYMOND
Revision Rev 0.1		

Data Protection Policy

Author	Published Date	Review Frequency
Katie Daniels	25/04/2018	Yearly
Approved By Kelvin Daniels	**Review Date** 25/04/2019	

Document History

Revision History

Revision Number	Summary of Changes	Author	Review Date	Approved By

Approvals

This document requires the following approvals:

Name	Title
Katie Daniels	Director
Kelvin Daniels	Managing Director

Distribution

This document has been distributed internally within Guy-Raymond.

1 Introduction

Guy-Raymond Engineering Company Limited (the "Company"). In the context of the General Data Protection Regulation (GDPR) we are a data controller for information we collect and a data processor for the data we process on behalf of others. The Company is aware of its obligations under the GDPR and is committed to processing any personal information securely and transparently.

2 Scope

This policy applies to all staff, which for these purposes includes employees, temporary and agency workers and other contractors. All staff must be familiar with this policy and comply with its terms. This policy applies to all personal data processed by the Company and held electronically or manually.

3 Roles and Responsibilities

Department	Responsibilities
Data Controller	The Company is a data controller under the terms of the legislation. This means it is ultimately responsible for controlling the use and processing of the personal data.
Data Protection Champion	The Company has appointed Data Protection Champions. They are responsible for data protection compliance within those areas. Questions about this Policy, or requests for further information, should be directed towards them. Please see the Data Protection Champions contacts list in Appendix B.
Data Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.

4 Policy Statement

4.1 Principles

The Company has adopted the following principles to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

4.1.1 Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner in relation to the Data Subject. This means, the Company must tell the Data Subject what Processing will occur (transparency), the Processing must match the description given to the Data Subject (fairness), and it must be for one of the purposes specified in the applicable Data Protection regulation (lawfulness).

4.1.2 Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This means the Company must specify exactly what the Personal Data collected will be used for and limit the Processing of that Personal Data to only what is necessary to meet the specified purpose.

4.1.3 Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. This means the Company must not store any Personal Data beyond what is strictly required.

4.1.4 Accuracy

Personal Data shall be accurate and, kept up to date. This means the Company must have in place processes for identifying and addressing out-of-date, incorrect and redundant Personal Data.

4.1.5 Storage Limitation

Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data is processed. This means the Company must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

4.1.6 Integrity and Confidentiality

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, and against accidental loss, destruction or damage. The Company must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data is maintained at all times.

4.2 Rights of Access

4.2.1 Data Subject Rights

Data subjects have the right of access to information held by the Company, subject to the provisions of the General Data Protection Regulations. Any data subject wishing to access their personal data should put their request in writing to the Data Protection Champion Lead. For more information on this please see the Subject Access Request Business Process Guide.

4.2.2 Response Requirements

The Company will normally respond to a request within a period of one month from the date it is received. In some cases, such as where the Company processes large amounts of the individual's data, it may respond within three months of the date the request is received. The Company will write to the individual within one month of receiving the original request to tell him/her if this is the case.

4.2.3 Request Exceptions

If a subject access request is manifestly unfounded or excessive, the Company is not obliged to comply with it. Alternatively, the Company can agree to respond but will charge a fee, which will be based on the administrative cost of responding to the request. A subject access request is likely to be manifestly unfounded or excessive where it repeats a request which the Company has already responded.

4.2.4 Data Security

The Company takes the security of personal data seriously. All staff and authorised third parties must follow the internal policies and controls that are in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties.

4.3 Data Breaches

If the Company discovers that there has been a breach of personal data that poses a risk to the rights and freedoms of individuals, it will conduct a risk assessment and where applicable report it to the Information Commissioner's Office within 72 hours of discovery. All individuals are responsible for reporting data breaches. For more information on data breaches please see the Data Breach Business Process Guide.

4.4 Data Retention

The Company will not retain personal data longer than is necessary in relation to the purposes for which it was originally gathered.

4.5 Data Sharing

The Company will only share personal data it where it is necessary. We will follow a due diligence process and make sure there is a contractual agreement to ensure the Regulations are followed. The third parties will let us know of any incidents relating to personal information. If data is going outside the European Economic Area (EEA) we will ensure there are adequate controls in place equivalent to the UK.

4.6 Privacy by Design

To ensure that all Data Protection requirements are identified and addressed when designing new systems or processes and/or when reviewing or expanding existing systems or processes a Data Protection Impact Assessment (DPIA) must be conducted. This is detailed in the project management methodology within Programme Delivery.

4.7 Consent

There are some circumstances where the processing of personal data is based on consent. In these cases we have processes in place to ensure consent is given explicitly and provide a simple method to withdraw their consent at any time.

4.8 Accuracy of Data

The Company will endeavour to ensure that all personal data held in relation to all data subjects is accurate. Data subjects must notify the relevant department of any changes to information held about them. Data subjects have the right in some circumstances to request that inaccurate information about them is erased. This does not apply in all cases, for example, where records of mistakes or corrections are kept, or records which must be kept in the interests of all parties to which they apply.

4.9 Privacy Notices

For transparency, the Company has detailed the reasons for processing personal data, how the Company uses such data and the legal basis for processing in its Privacy Notices. The Company will not use personal data of individuals for other reasons. Where the Company relies on legitimate interests as the basis of processing data, it will carry out an assessment to ensure those interests are not overridden by the rights and freedoms of individuals.

4.10 Compliance Monitoring

4.10.1 Compliance Audit

To confirm this Policy has been implemented and that there is an adequate level of compliance being achieved by all areas of the Company an annual audit will be conducted. This may result in implementing corrective actions to achieve the required level of Compliance.

4.10.2 Breach of Policy

Any breach of the Data Protection Policy may lead to disciplinary action being taken, or a withdrawal of a contract, or even criminal prosecution. Any questions or concerns about the interpretation or operation of this Policy should be taken up with the designated Data Champion.

Appendix A - Definitions

Term	Definition
Personal Data	Any information (including opinions and intentions) which relates to an identified or identifiable Natural Person.
Special Categories of Data	Personal Data pertaining to or revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership; data concerning health or sex life and sexual orientation; genetic data or biometric data.
Process, Processed, Processing	Any operation or set of operations performed on Personal Data or on sets of Personal Data, whether or not by automated means. Operations performed may include collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Confidential Information	Personal Data and Special Categories of Data as defined above are types of information which is classed as confidential. Non-person-identifiable information can also be classed as confidential information e.g. financial reports; commercially sensitive information e.g. contracts, trade secrets, procurement information.
Data Subject	The identified or identifiable natural person to which the data refers.
Data Controller	A natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Champion	The Company has appointed Data Protection Champions. They are responsible for data protection compliance within those areas. Questions about this Policy, or requests for further information, should be directed towards them. Please see the Data Protection Champions contacts list in Appendix B.
Data Processors	A natural or legal person, public authority, agency or other body which processes personal data on behalf of a data controller.
Third Party	A natural or legal person, public authority, agency or other body which under the direct authority of the controller or processor, are authorised to process personal data.

Appendix B

Data Protection Controller

Name	Department	Email	Phone
Katie Daniels	Director	katiedaniels@guy-raymond.co.uk	816034

Data Protection Champions

Name	Department	Email	Phone
Kelvin Daniels	Managing Director	kelvindaniels@guy-raymond.co.uk	816049
Katie Daniels	Director	katiedaniels@guy-raymond.co.uk	816034
David Whittaker	Compliance	Metchem10@gmail.com	