INTRODUCTION

Ridge and Partners LLP provides a full range of professional, multi-discipline property and construction consultancy services for all market sectors, across the UK and around the world. Ridge and Partners LLP needs to gather and use certain information about individuals. These can include its equity partners, customers, suppliers, business contacts, and other people the organisation has a relationship with or may need to contact while carrying out its legitimate business.

Ridge and Partners LLP must comply with the principles of the General Data Protection Regulation (GDPR) 2016, which came into force on 25th May 2018.

In summary, these regulations state that personal data shall:

- Be obtained and processed fairly and lawfully, and shall not be processed unless certain conditions are met.
- Be obtained for a specified, explicit and legitimate purpose and shall not be processed in any manner incompatible with that purpose.
- Consent must be obtained before obtaining and processing specific categories of data: race, ethnic origin, politics, religion, health, disability or sexual orientation.
- Be adequate, relevant and limited to what is necessary for that purpose.
- Be accurate and kept up to date.
- Not be kept in a form which permits identification of individuals, for any longer than is necessary for the purpose for which it is stored. Individuals have the right to request that personal data is removed once the purpose for which it was obtained has ceased.
- 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, using appropriate technical or organisational measures.
- Be kept safe from unauthorised access, accidental loss or destruction.
- Not be transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.
This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards – and to comply with the law.

The wholly owned subsidiary, Ridge Surveyors Limited is the employing entity; employee data is gathered and processed by Ridge Surveyors Limited and is covered in a separate policy.

Policy Scope

This policy applies to:

- All branches of Ridge and Partners LLP
- All individuals working on behalf of Ridge and Partners LLP, whether engaged directly as suppliers of professional services, or as employees of Ridge Surveyors Limited.

It applies to all personal data that the company holds relating to identifiable individuals, This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- Plus any other information relating to individuals

Responsibilities

Everyone who works on behalf of Ridge and Partners LLP has some responsibility for making sure that personal data is collected, stored and handled appropriately.

Each team that handles personal data must make sure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The Equity Partners are ultimately responsible for making sure that Ridge and Partners LLP meets its legal obligations.

The Ridge and Partners LLP designated data controller is responsible for:

- Keeping the Partners updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies.
- Arranging data protection guidance for the people covered by this policy.
- Handling data protection questions from anyone covered by this policy.
- Dealing with requests from individuals to see the data Ridge and Partners LLP hold about them (also called "subject access requests").
- The designated Data Controller is David Walsh, QA Manager.

The Partner responsible for IT is responsible for:

- Making sure that all systems, services and equipment used for storing personal data meet acceptable security standards in accordance with the guidance provided in Article 32 of the GDPR, and appropriate to the risk. This has been achieved by putting in place an IT system that complies with Cyber Essentials Plus standards as recommended by the UK Government National Cyber Security Centre, and which is independently audited as part of the accreditation process.

The Partner responsible for Marketing is responsible for:

- Making sure that data protection statements explaining why personal data is gathered and how it is used are provided and attached to communications such as emails and letters, forms or other methods of collecting personal data, and the company web site.
- Addressing any data protection queries from other staff to make sure that marketing initiatives abide by data protection principles.

The Partner responsible for Administration is responsible for:

- Making sure that personal data required to process payments and invoice clients is gathered held and processed in accordance with the principles of the GDPR
- That personal data is held only for as long as is necessary for financial reporting purposes

Data Storage

These rules describe how and where personal data should be safely stored:

- When personal data is stored on paper, it should be kept in a secure place where unauthorised people cannot see it.
- These guidelines also apply to personal data that is usually stored electronically but has been printed out for some reason:
- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Care should be taken to make sure paper and printouts are not left when unauthorised people could see them, like on a printer.

- Data printouts containing personal information should be shredded and disposed of securely when no longer required.
- When personal data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Personal Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If personal data is stored on removable media (like a CD or DVD), these should only be uploaded to an approved cloud computing services.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Personal Data should never be saved directly to laptops or other mobile devices like tablets or smart phones, unless they are provided by the Partnership, administered by RT Systems, and are protected by approved security software.
- All servers and computers containing personal data should be protected by approved security software and a firewall.

Data Use

- When working with personal data employees should make sure that the screens of their computers are always locked when left unattended.
- Personal data should not be shared informally. When personal data is sent by email it should be in a password protected document attached to the email rather than within the body of the email itself, as this form of communication if not secure. Additional protection can be given to personal data sent by email if the email is flagged as "private".
- Personal data should only be gathered if it is required to carry out a legitimate business task. No more personal data should be gathered than is absolutely necessary or relevant to that task. Consent must be obtained to gather and use the information, and it must be deleted or destroyed once the purpose for which it was given has ceased.

Data Accuracy

- It is the responsibility of all employees who work with personal data to take reasonable steps to make sure that it is kept as accurate and up to date as possible.
- Personal data will be held in as few places as necessary. Staff should not create any unnecessary additional data sets.
- Staff should take every opportunity to make sure that that personal data is updated. For instance, by confirming a customer's details when they call.
- Personal data should be updated as inaccuracies are discovered. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.

Subject Access Requests

All individuals who are the subject of personal data held by Ridge and Partners LLP are entitled to:

- Ask what information the company holds about them and why
- To be given access to any personal data held relating to them.
- Be informed how to keep it up to date.

If a client or other individual contacts the company requesting this information, this is called a "subject access request". Subject access requests from individuals should ideally be made by email to the Data Controller at privacy@ridge.co.uk. The Data Controller will provide the relevant data within 30 days.

The Data Controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing Data for Other Reasons

In certain circumstances, the Data Protection Act allows personal data to be disclosed to law enforcement agencies without the consent of the data subject. Under these circumstances, Ridge and Partners LLP will disclose requested data. However, Ridge and Partners LLP will make sure that the request is legitimate, seeking guidance from legal advisers where necessary.

Types of data held and what we do with it

The types of data held by Ridge and Partners LLP relates to our clients and suppliers, and is likely to include as a minimum, names, addresses phone numbers and email addresses of clients, and on some occasions of tenants occupying buildings owned or managed by our clients. This information is necessary for us to carry out survey work, or other work relating to our core business activities. We will hold data sufficient for us to invoice or to pay our clients and suppliers, to contact them regarding on going work, and to make them aware of any developments in the services offered by Ridge and Partners LLP.

Ridge and Partners LLP holds and processes confidential personal data relating to contractors and sub consultants who carry out work on behalf of Ridge, limited to what is necessary to process payments and carry out security checks and other checks as and when required by our clients.

Ridge and Partners LLP holds confidential personal information relating to the Equity Partners as required to meet its obligations in accordance with the partnership agreements.

Data Retention

Data collected and held in relation to specific client projects will be retained by Ridge indefinitely. Data collected for the purpose of invoicing or paying clients and suppliers will be retained for financial reporting purposes for a period of 7 years. Client contact data will be updated regularly, and any client data not required as part of the project records, will not be kept once the reason for which it was required as ceased. Data required to process and make payments to Equity Partners and Sub Consultants will be retained for financial reporting processes for a period of 7 years after the termination of relevant agreements. Ridge and Partners LLP will comply with any "requests to be forgotten" provided that it is possible to do so and continue to meet the requirement for which the data was legitimately obtained and held.

Conclusion

Compliance with the GDPR is the responsibility anyone who works with personal data on behalf of Ridge and Partners LLP. The Requirement to comply also extends to RT Systems who are contracted to supply and maintain IT solutions and equipment on which sensitive personal data is held and processed. Any deliberate breach of the data protection policy may lead to disciplinary action being taken, or even to a criminal prosecution. Any questions or concerns about the interpretation or operation of this policy should be taken up with the Designated Data Controller.

Signed:  .....

Adrian O'Hickey, Partner
Date: 15 May 2019