



Data Protection Act 2018 (Part 2 Chapter 2)

GENERAL DATA PROTECTION REGULATION POLICY 2018

Issue No: - 01

Review Date - May 2019

	<i>Issued By: Deborah Kilpatrick</i>	<i>QSD 67</i>	<i>Issue Date: 25.05.18 Revision: 1</i>
General Data Protection Regulations Policy		<i>Approved By: Clive Kilpatrick</i>	

Table of Contents

1.0 What is GDPR?.....2

2.0 Definitions2

3.0 What information does the GDPR affect?2

3.1 What constitutes as data?3

4.0 How does it affect Our Company?3

5.0 What are the changes to the Data Protection Act 1998?3

6.0 What are the six principles of GDPR?5

7.0 Our Company Process..... 5

7.1 How we handle, retain and store the information provided6

8.0 DECLARATION.....7

APPENDIX 1 – PRIVACY STATEMENT.....8

	Issued By: Deborah Kilpatrick	QSD 67	Issue Date: 25.05.18 Revision: 1
	General Data Protection Regulations Policy		Approved By: Clive Kilpatrick

1.0 What is GDPR?

The EU General Data Protection Regulation (GDPR) came into force on 25 May 2018 under the umbrella of the Data Protection Act 2018, Part 2, Chapter 2.

We understand that GDPR is an EU-wide regulation that will replace the current data protection laws in the UK. It has been designed to provide greater protection for personal data in today's digital world.

We understand that getting GDPR wrong is not an option. These fines could bankrupt our business with fines for non-compliance or data breaches of up to €20m, or four per cent of global turnover – whichever is greater.

We also understand that Brexit will not affect the commencement of the GDPR. The UK Government has made it clear that GDPR is part of UK law, as it also applies to companies who interact with citizens of other EU countries.

2.0 Definitions

Data subject – this is a term used to refer to an individual whose personal information is the data in question.

Processing – this refers to the collection, storing and transferring of personal data.

Profiling – this is something that is often done by larger companies and involves automatic processing of personal information (often in large batches) to evaluate aspects of the individuals' behaviour and make decisions or take actions.

ICO – the Information Commissioner's Office is the UK's independent authority set up to uphold information rights in the public interest. In the Republic of Ireland, the Data Protection Commissioner holds a similar position.

Data Controller – this is the person in an organisation that decides what data is collected, what it is used for and who it is shared with.

Senior Information Rights Owner (SIRO) – this is usually a board-level role to oversee data policies.

Data Protection Officer – this role is required in certain circumstances, such as public authorities and companies dealing with sensitive data – **Not Required**

Data Processor – this refers to anyone, sometimes a third- party organisation or business (e.g. printing company), who processes data on the instruction of the Data Controller.

3.0 What information does the GDPR affect?

We understand that GDPR applies to the handling and storing of any personal data that could be used directly or indirectly to identify a person. GDPR applies to both automated personal data and to manual filing systems.

	<i>Issued By: Deborah Kilpatrick</i>	<i>QSD 67</i>	<i>Issue Date: 25.05.18 Revision: 1</i>
General Data Protection Regulations Policy		<i>Approved By: Clive Kilpatrick</i>	

3.1 What constitutes as data?



Personal data – any information which relates directly to an individual and can be linked directly to them. This includes a person’s name, phone number, email address, photographs, genetic and economic data. **This kind of data is the focus of GDPR and data protection.**



Anonymous data – data which has been anonymised properly cannot be traced back to the original individuals in any way but can still be processed by companies to conduct research. Fully anonymous data is not covered by GDPR as it contains no personal information to protect.



Pseudonymous data – data which has been properly pseudonymised can only be connected back to an individual using a specific ‘key’ or code. This can be an extra layer of security, but the data is still treated as Personal Data under GDPR because of the possibility of personal identification

Like the existing Data Protection Regulation, GDPR refers to ‘data controllers’ and ‘data processors’.

4.0 How does it affect Our Company?

GDPR details procedures that are required by law, so we need to comply with them.

It is therefore essential to make sure that we – as a contractor, or a supplier of goods or services are following best practice in terms of:

- **how we gather information**
- **how securely we store information**
- **how we comply with reasonable requests for the information we hold**
- **how we can provide evidence of any of the above**

Ensuring that we have clear policies and acceptable processes in place will give us a strong case against a hefty fine in the event of non-compliance or data breach.

5.0 What are the changes to the Data Protection Act 1998?

GDPR has focused on the large fines but, in practice, some of the most significant changes that will affect how we all work is in the additional rights afforded to individuals. These allow individuals to request access, corrections and removal of their personal information in ways that weren’t available before. These are expressed as rights.

The new regulation requires clearer evidence of consent from individuals and some methods of recording consent will no longer be valid. We must have a legal basis for processing an individual’s data and understand that they have certain rights: -

Key	Data Rights	Process	Actions
	RIGHT TO BE INFORMED	Interested Parties should be informed of how their data is collected, stored and processed in a clear, accessible way	We will provide this in our Privacy Statements, which will be available on our website and on request
	RIGHT OF ACCESS	Interested Parties can request access to a copy of their data in electronic form and details of how it is processed	We should provide this, for free, within one month
	RIGHT TO RECTIFICATION	Interested Parties can request to have their data rectified if it is incorrect	We should provide this within one month, two if it is a particularly complex task
	RIGHT TO ERASURE	Also known as 'the right to be forgotten', this permits Interested Parties to request the deletion of their data	We must do this within one month, unless we have a strong, valid reason – dependent on the information and storage requirements of other parties – Inland Revenue/VAT
	RIGHT TO RESTRICTION OF PROCESSING	Interested Parties can request a halt on processing if they object to accuracy or purpose, but we can still hold the data until resolved	This will be a temporary stop until the matter is investigated. The Interested party will be kept informed of each step of the investigation
	RIGHT TO OBJECT	Allows Interested Parties to obtain and reuse their data for their own purposes	We must provide the information in a structured, commonly used and machine-readable form. And we must be able to send this within one month.
	RIGHT TO DATA PORTABILITY	Interested Parties can, in certain cases, object to the processing of their data, e.g. in direct marketing	We only pass information onto third parties who have a legitimate interest in the data. We will make the assumption that these third parties are operating under the GDPR legislation.
	RIGHTS IN RELATION TO AUTOMATED DECISION MAKING	Interested Parties can object to potentially damaging decisions being taken against them, based only on automated data processing	The company does not use automated data processing

	<i>Issued By: Deborah Kilpatrick</i>	<i>QSD 67</i>	<i>Issue Date: 25.05.18</i> <i>Revision: 1</i>
	General Data Protection Regulations Policy		<i>Approved By: Clive Kilpatrick</i>

6.0 What are the six principles of GDPR?



Lawfulness, fairness and transparency – this covers the primary areas of concern that data should be gathered and used in a way that is legal, fair and understandable. The public has the right to know what is being gathered and have this corrected or removed.



Purpose limitation – We should only use data for a legitimate purpose specified at the time of collection. This data should not be shared with third parties without permission.



Data minimisation – the data collected by our company should be limited only to what is required for the purpose stated. We should not collect data without purpose.



Accuracy – the personal data we hold should be accurate, kept up-to-date, and if it is no longer accurate, it should be rectified or erased.



Storage limitation – personal data should only be stored for as long as is necessary. Data can be archived securely and used for research purposes in the future. Where possible, the personally identifiable information should be removed to leave anonymous data.



Integrity and confidentiality – personal data should be held in a safe and secure way that takes reasonable steps to ensure the security of this information and avoid accidental loss, misuse or destruction.

7.0 Our Company Process

We believe that privacy is a very important right for everyone and we wish to assure all the company's customers/personnel/clients/subcontractors etc. (known as **"Interested Parties"**) that we are working hard on ensuring compliance on all areas of the business.

We want to highlight to our Interested Parties the measures we have put in place to ensure compliance with the GDPR where we hold or process data and to raise our awareness of the measures we need to comply with on our behalf.

GENERAL DATA PROTECTION REGULATIONS CONTROL MEASURES	
Data Subject Rights	<p>We will work with Interested parties for whom we hold or process personal data to determine how best to facilitate:</p> <ul style="list-style-type: none"> • Handling data subject access requests and rectification of personal data • The application of retention periods and the secure erasure and destruction of personal data • Responding to data portability requests, providing it in a structured, commonly used and machine-readable format
Data Protection Officer and data controllers and processors	<p>We do not need to appoint a Data Protection Officer</p> <p>Trueline Surveys are a Data Controller - We will take full responsibility for all matters relating to data protection and GDPR compliance.</p> <p>As Data Processors - we will ensure that we are accountable and transparent to the supervisory authorities, including the creation and maintenance of "Records of processing activities for controllers and processors" as per Article 30 of the GDPR.</p>



GENERAL DATA PROTECTION REGULATIONS CONTROL MEASURES

Data breaches	<p>Under the GDPR, we must notify any data breach to the controller without undue delay. We therefore have processes and procedures in place to identify, review and promptly report data breaches to the relevant controller.</p> <p>As a processor of our company data we would need to provide the controller with:</p> <ul style="list-style-type: none"> - A description of the nature of the breach - Contact details of the responsible data protection officer or any other contact person - Details of the likely consequences of the data breach - Proposed and imposed measures that we have taken to limit harmful effects <p>We would stress again that we have comprehensive technical and organisational security measures in place to mitigate against a data breach.</p>
Privacy statement	<p>We have updated our privacy statement to reflect the new rules. The purpose of this statement is to provide individuals with further information on the collection of data, how long it is retained, the purpose of the collection of data and how it is obtained (consent), plus the sharing of data with any third-parties or international transfers.</p>
Security and business continuity measures	<p>We continually seek to ensure the confidentiality, integrity and availability of the personal data we store or process. We maintain appropriate technical and organisational security measures to protect personal data against accidental or unlawful destruction or loss, alteration, unauthorised disclosure or access.</p>
Interested Parties Contracts	<p>GDPR requires that a data controller must appoint data processors who have undergone GDPR training and will adhere to the Regulations in relation to the contract process. We will be reviewing our contracts with all our Interested Parties to ensure compliance. This will ensure that relevant wordings are in place to cover aspects such as the duration, nature and purpose of the processing, the types of data processed and the obligations and rights of the Data controller. It will also, where applicable, cover cross-border transfers and the use of any sub-processors.</p>

7.1 How we handle, retain and store the information provided

We have produced **GDPR Controller/Processor Record Handling Grid** this has been adapted to include the requirements of Article 6 of the Data Protection Act 2018 (lawful basis), Article 9 (basis for processing special category data (employment) etc. Article 30 of the GDPR are compulsory requirements and will be contained within this document. This is a controlled document which will be handled by one of our Internal Data Processors – **Deborah Kilpatrick**.

	<i>Issued By: Deborah Kilpatrick</i>	<i>QSD 67</i>	<i>Issue Date: 25.05.18 Revision: 1</i>
General Data Protection Regulations Policy		<i>Approved By: Clive Kilpatrick</i>	

8.0 DECLARATION

Our company intends to comply with the General Data Protection Regulations 2018 to the best of our ability the persons who will be involved in the compliance with this Policy are:

***Clive Kilpatrick - Director – Data Controller
Deborah Kilpatrick – Data Processor***

These persons have: -

- Reviewed our current security and privacy processes and where applicable, revised our contracts with interested parties to meet the requirements of the GDPR
- Identified the Personally Identifiable Information (PII) and personal data that is being collected
- Analysed how this information is being processed, stored, retained and deleted
- Assessed the interested parties with whom we disclose data
- Established procedures to respond to data subjects when they exercise their rights
- Established and conducted a Privacy Impact Assessment (PIA)
- Created processes for data breach notification activities
- Continuous employee awareness is vital to ensure continual compliance to the GDPR

Signed _____
Clive Kilpatrick, Director

Dated 25th May 2018



	<i>Issued By: Deborah Kilpatrick</i>	<i>QSD 67</i>	<i>Issue Date: 25.05.18 Revision: 1</i>
General Data Protection Regulations Policy		<i>Approved By: Clive Kilpatrick</i>	

APPENDIX 1 – PRIVACY STATEMENT

1.0 Introduction

The General Data Protection Regulations forms part of the Data Protection Act 2018, Part 2, Chapter 2 and we aim do our best to protect and respect your personal data. This statement explains how we collect that data, why we use it and how we keep it safe.

2.0 Who are we?

Trueline Surveys, Land Surveying Services. Our office is at Branford House, 5 Cladymore Rd, Mowhan, Armagh BT60 2EW Tel: 028 37508180. For general queries, contact info@truelinesurveys.co.uk For queries in relation to data protection, email info@truelinesurveys.co.uk

3.0 How do we collect your information?

We obtain information about you when you make contact with us. For example, when you join our company, supply us with materials, consult with us on our projects, supply us with sub-contracting services.

4.0 What types of information do we hold?

The information we collect might include your name, address, email address and phone numbers, bank details, date of birth, National Insurance Number, your signatures, medical information, details of any criminal records etc. We will store this information in order to comply with other statutory legal functions/legitimate interests such as HMRC – PAYE/CIS requirements; Health and Safety – health reasons and possible litigation in the future.

5.0 Why do we collect your information?

We only use your information in accordance with the law and performing normal business functions such as auditing accounts etc. This gives us various powers to use your data. These are effectively the reasons for our processing and are:

- ✓ **To perform or take steps to enter a contract with you.**
- ✓ **For the purposes of our legitimate interests. This includes being able to ensure safety on site and allow payments to be made to you.**
- ✓ **Compliance with a legal obligation.**

Collecting and using your data will mean we are able to pay salaries, process any orders or requests third parties may have and to provide you with information relating to your interests.

6.0 Who has access to your information?

Staff of Trueline Surveys will have controlled access to your information to enable us to carry out our day to day functions together with any specific interests you may have with the Company. We will not sell or rent your information to third parties. We will not share your information with third parties for them to send marketing to you. We may pass your information to our third-party service providers, subcontractors and other associated organisations to provide services on our behalf (for example HMRC). However, when we use third parties, we

	<i>Issued By: Deborah Kilpatrick</i>	<i>QSD 67</i>	<i>Issue Date: 25.05.18 Revision: 1</i>
General Data Protection Regulations Policy		<i>Approved By: Clive Kilpatrick</i>	

disclose only the personal information that is necessary to deliver the service and we require them to keep your information secure and not to use it for their own direct marketing purposes.

7.0 *Your Choices*

You have a choice about whether and how you wish to receive information from us. You will be asked to make your preferences clear when we collect your information. For most users, this will be when they join the company or enter into a contract with the company. Your preferences can be updated at any point. The accuracy of your information is important to us. Please do regularly check and update your information with our Company.

You have various legal rights over your information which we will always respect. Further detail is available from the Information Commissioner. www.ico.org.uk

8.0 *How do we protect your data?*

We take several steps to protect your data. This includes robust IT security. All staff receive data protection training and our premises are secured. We have contracts with IT providers requiring them to protect your information. If we transfer your data outside of the EU we will ensure that extra checks are in place for the cross-border transfer of information.

9.0 *How long will we hold your personal Information?*

We will only keep your personal information for as long as it is necessary for as long as it is necessary to comply with applicable laws. In most cases this will be six years from the date the information is gathered. After this period, we will securely destroy your personal data. The exception to this will be under medical grounds which requires that we hold information for 40 years.

10.0 *Your rights in connection with personal information?*

Under certain circumstances, by law you have the right to:

- ✓ ***Request access to your personal information***
- ✓ ***Request correction of personal information that we hold about you***
- ✓ ***Request erasure of your personal information***
- ✓ ***Object to processing of your personal information***
- ✓ ***Request the restriction of your personal information***
- ✓ ***Request the transfer of your personal information to another party***

If you have any questions about this privacy notice or how we handle your information, please email info@truelinesurveys.co.uk or telephone – 028 37508180

Signed _____

Clive Kilpatrick, Director



Date 25th May 2018