Review Date: Reviewed May 2018 Author: Alex Bell
Active from: 25th May 2018

General Data Protection Regulation Policy

Foreword

During our work we will come into contact with or use 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This personal data can be about employees, clients, customers, suppliers and subcontractors. We have policies and processes in place to ensure that we comply with legal regulations and that we operate to best practice standards in relation to using and storing personal data. In addition to this Data Protection Policy we also have policies in force relating to cyber security and employee conduct.

The General Data Protection Regulation (GDPR) (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area that became enforceable on the 25th May 2018.

The purpose of policy is to assist Courtcraft in its compliance GDPR regulations.

GDPR Definitions & Principles

The Courtcraft GDPR Policy applies to 'controllers' and 'processors' in Courtcraft.

A controller determines the purposes and means of processing personal data.

A processor is responsible for processing personal data on behalf of a controller.

Courtcraft Processors are all employees who will use personal data to be able to undertake their job.

The courtcraft data controller is Alex Bell (Business manager). If you need to contact Courtcraft in relation to Data Protection and how we use personal data, then please write to:

Courtcraft limited
Logic house
31 Gibfield park avenue
Gibfield business park
Atherton
Manchester
M46 0SY

or email: equiries@courtcraft.co.uk

The GDPR applies to processing carried out by organisations operating within the EU. It also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The GDPR does not apply to certain activities including processing covered by the Law Enforcement Directive, processing for national security purposes and processing carried out by individuals purely for personal/household activities.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

Article 5 of the GDPR sets out seven key principles:

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');

(f) 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 ('integrity and confidentiality')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

For Courtcraft to process personal data we must have a valid lawful basis to do so:

There are six available lawful bases for processing. No single basis is 'better' or more important than the others – which basis is most appropriate to use will depend on our purpose and relationship with the individual. Most lawful bases require that processing is 'necessary'. If we can reasonably achieve the same purpose without the processing, we will not have a lawful basis.

If our purposes change, we may be able to continue processing under the original lawful basis if our new purpose is compatible with our initial purpose (unless your original lawful basis was consent).

The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever we process personal data:

(a) Consent: the individual has given clear consent for us to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract we have with the individual, or because they have asked us to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for us to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone's life.

(e) Public task: the processing is necessary for us to perform a task in the public interest or for our official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for our legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

Personal data use and your rights

We use personal data for the following purposes:

Receiving services or products

We process personal data in relation to our suppliers and their staff as necessary to receive the services. For example, where a supplier is providing us with services, we will process personal data about those individuals that are providing services to us.

Providing professional services or products to clients

Where we provide services to clients and customers we process personal data about the individuals involved in providing the services to administer and manage our relationship with the clients or customers

Where a supplier is helping us to deliver services to our clients, we process personal data about the individuals involved in providing the services to administer and manage our relationship with the supplier and the relevant individuals and to provide such services to our clients.

Administering, managing and developing our businesses and services

We process personal data to run our business, including:

- managing our relationships with clients or customers
- fulfilling our contractual obligations with clients or customers
- managing our relationship with suppliers
- developing our businesses and services

Security, quality and risk management activities

We have security measures in place to protect our and our clients' information, including personal data which involve detecting, investigating and resolving security threats. Personal data may be processed as part of the security monitoring that we undertake; for example, automated scans to identify harmful emails. We have policies and procedures in place to monitor the quality of our services and manage risks in relation to our suppliers. We collect and hold personal data as part of our supplier and client contracting procedures. We monitor the services provided for quality purposes, which may involve processing personal data.

We are subject to legal, regulatory and professional obligations. We need to keep certain records to demonstrate that our services are provided in compliance with those obligations and those records may contain personal data.

Data retention

We retain the personal data processed by us for as long as is considered necessary for the purpose for which it was collected (including as required by applicable law or regulation).

Personal data may be held for longer periods where extended retention periods are required by law or regulation and to establish, exercise or defend our legal rights.

Personal data held by us may be transferred to

Third party organisations that provide applications/functionality, data processing or IT services to us.

We use third parties to support us in providing our services and to help provide, run and manage our internal IT systems. For example, providers of information technology, cloud-based software as a service provider, website hosting and e-mail management, data back-up, security and storage services. The servers powering and facilitating that cloud infrastructure are all certified to gold-standards eg ISO 27001 for physical and cyber-security.

Auditors and other professional advisers

Law enforcement or other government and regulatory agencies or to other third parties as required by, and in accordance with, applicable law or regulation.

Occasionally, we may receive requests from third parties with authority to obtain disclosure of personal data, such as to check that we are complying with applicable law and regulation, to investigate an alleged crime, to establish, exercise or defend legal rights. We will only fulfil requests for personal data where we are permitted to do so in accordance with applicable law or regulation.

Individuals' rights and how to exercise them

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access (Individuals can make a subject access request verbally or in writing)
- The right to rectification (An individual can make a request for rectification verbally or in writing)
- The right to erasure, also known as 'the right to be forgotten' (Individuals can make a request for erasure verbally or in writing)
- The right to restrict processing
- The right to data portability, allows individuals to obtain and reuse their personal data for their own purposes across different services
- The right to object (Individuals have an absolute right to stop their data being used for direct marketing)
- Rights in relation to automated decision making and profiling.

Amendment of personal data

To update personal data submitted to us, you may write to us.

When practically possible, once we are informed that any personal data processed by us is no longer accurate, we will make corrections (where appropriate) based on your updated information.

Withdrawal of consent

Where we process personal data based on consent, individuals have a right to withdraw consent at any time.

Complaints

We hope that you won't ever need to, but if you do want to complain about our use of personal data, please send write to us. We will look into and respond to any complaints we receive.

You also have the right to lodge a complaint with the Information Commissioner's Office ("ICO") (the UK data protection regulator). For further information on your rights and how to complain to the ICO, please refer to the ICO website **www.ico.org.uk** .