GDPR/Data Protection Act 2018

Handbook

Updated: May 2024

Contents

Purpose of this Document

This document is a reference point for all to use for queries regarding data protection. It summarises the key areas of the General Data Protection Regulation/Data Protection Act 2018 and how we comply. This policy outlines how we collect, process, store, and handle personal data in compliance with the GDPR. This document is for internal use only.

Context and Overview

Introduction

The EU's General Data Protection Regulation (GDPR) is the culmination of efforts to update data protection for the 21st century, in which people regularly grant permissions to use their personal information for a variety of reasons, including for the provision of services.

The Data Protection Act 2018 (DPA 2018) is the UK's implementation of the General Data Protection Regulation (GDPR) and has replaced the Data Protection Act 1998, which was brought into law to implement the 1995 EU Data Protection Directive. GDPR/DPA 2018 gives individuals more control over how organisations use their data, and introduces penalties for organisations that fail to comply with the rules and for those that suffer data breaches. It also ensures data protection law is almost identical across the EU.

Definitions

- Personal data: refers to any information relating to an identified or identifiable individual. The definition of personal data from GDPR/DPA 2018 is as follows:

  'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

- **Data Controller:** A Data Controller is a person/business which, alone or jointly, determines the purposes and means of processing personal data.

- **Data Processors:** A person/business which processes personal data on behalf of the controller for example, an administration centre or a self-employed Adviser.

- **Data Subjects:** a living individual to whom personal data is being collected, processed, or stored. A data subject can be a client, or employee.

- **Processing:** refers to any operation performed on personal data, such as collection, recording, storage, use, disclosure, or deletion, whether or not by automated means.

The Data Protection Officer (DPO)

Nicholas Standeven oversees internal compliance and monitoring. For any queries, contact nstandeven@crossley.uk.com

Questions and Concerns

If you have any questions on how personal data should be processed lawfully and concerns of any wrongdoings or inappropriate personal data processing; please contact the DPO confidentially by email.

Lawfulness, fairness and transparency

Introduction

We have an obligation under GDPR/DPA 2018 to ensure that personal data is processed lawfully, fairly and in a transparent manner in relation to individuals. This section of the handbook outlines what's needed to confirm that data is being processed lawfully.

Data collection and consent

We will only collect personal data that is necessary for the provision of our accounting services or as required by law. Prior to collecting any personal data, we will obtain the explicit consent of the data subject, explaining the purpose and legal basis for processing their data.

Lawful bases for processing personal data

We will ensure that there is a lawful basis for processing personal data, as defined by the GDPR. This includes processing personal data for the performance of a contract, compliance with a legal obligation, protection of vital interests, consent, performance of a task carried out in the public interest, or legitimate interests pursued by our firm.

Data Security

We implement appropriate technical and organisational measures to protect personal data from unauthorised access, accidental loss, alteration, or disclosure. This includes encryption, restricted access controls, regular backups, and staff training on data protection practices.

Data Retention

We will retain personal data for no longer than necessary for the purposes it was collected, or as required by legal obligations. We will establish clear retention periods for different types of personal data and regularly review and securely dispose of data that is no longer needed.
Please see the FAQ's for information on time frames.

Data Subject Rights

We respect data subjects' rights as outlined in the GDPR, including the right to access, rectify, erase, restrict processing, object to processing, data portability, and not to be subject to automated decision-making. We will promptly respond to any requests from data subjects to exercise their rights.

Right to be informed and privacy notices

Individuals have the right to be informed about the collection and use of their personal data in a concise, transparent, intelligible and easily accessible manner. Individuals must be provided with information at the time you collect their personal data from them. This information includes your purposes for processing their personal data, retention periods for that personal data and with whom it will be shared.

Data Subject Access Requests

The right of access gives individuals the right to obtain a copy of their personal data as well as other supplementary information. It helps individuals to understand how and why Crossley & Co are using their data and check that we are doing it lawfully. In most circumstances we cannot charge a fee to deal with a request.

A request can be made verbally or in writing. Requests can be made to any part of the organisation (including by social media) and do not have to be to a specific person or contact point. A request does not have to include the phrase 'subject access request' or reference Article 15 of the GDPR as long as it is clear that the individual is asking for their own personal data.

We have a legal responsibility to identify that an individual has made a request to Crossley & Co and handle it accordingly. We have an obligation to respond to a request within one month.

I

Right to rectification and data quality

The rectification of data is not a new requirement and is typically undertaken on a day-to-day basis (e.g. change of address). Data subjects are entitled to have personal data corrected if it is inaccurate and/or incomplete.

Personal data should be corrected within one month of a request being received.

Right to erasure, including retention and disposal

Data subjects can request that their personal data is deleted when they feel there is no compelling reason for its continued use.

The right of erasure does not provide an absolute right to be forgotten. Individuals only have the right to have data removed under specific circumstances, for example:

- when a data subject withdraws consent (e.g. marketing activity).
- if the data was processed in breach of GDPR/DPA 2018.
- if it is no longer necessary to retain data in relation to its original purpose (e.g. a contract has been terminated).

Any data retained by Crossley & Co must meet the requirements of GDPR Article 5 (Principles relating to processing of personal data) and be limited to that which is necessary.

Right to restrict processing

Data subjects can request a block or suppression on processing of their personal data under certain conditions. Crossley & Co will restrict the processing of personal data if the data is inaccurate or is being processed unlawfully.

If data is under processing restrictions, it may only be stored.

Any data that is inaccurate must be corrected immediately; all other requests should be sent to the Data Protection Officer for processing.

Right of data portability

Data subjects can request their personal data be transferred to another controller when the personal data is:

- originally provided by the data subject (e.g. not transactional data), and
- processed with the consent of the data subject or needed for the performance of a contract, and
- automatically processed.

Any requests for data portability must be sent to the Data Protection Officer for processing.

Right to object
The GDPR/DPA 2018 gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing where processing is based upon consent.

Any objections must be sent to the Data Protection Officer for processing.

Rights related to automated decision-making, including profiling
For any system that relies on automated decision making and profiling, data subjects have the right to:

- be informed about the nature of the processing.
- request human intervention and challenge a decision.

Automated data processing and profiling are processes undertaken without any human interaction. Data processing and profiling can only be carried out where it is necessary to enter into contract or with the data subject's explicit consent. Any requests relating to automated decision making must be sent to the Data Protection Officer for processing.

Data Sharing and Third Parties
We will not share personal data with third parties unless it is necessary for the provision of our services, or when required by law. In such cases, we will ensure appropriate data protection agreements and safeguards are in place.

International Data Transfers
If we transfer personal data outside the European Economic Area (EEA), we will ensure that adequate safeguards are in place to protect the data, such as using standard contractual clauses or relying on the Privacy Shield framework if applicable.

Data Breach Notification
In the event of a personal data breach, we will promptly assess the risk to individuals and, if necessary, report the breach to the Information Commissioner's Office (ICO) and affected individuals within 72 hours of becoming aware of the suspected breach, in compliance with GDPR requirements.

Staff Training and Responsibility
We provide regular data protection training to our employees to ensure they understand their responsibilities under the GDPR. Nicholas Standeven is responsible for overseeing compliance with data protection laws and handling data protection inquiries.

Policy Review
We will review and update this GDPR policy periodically to ensure ongoing compliance with data protection laws and industry best practices.
If you have any questions or concerns about our GDPR policy or how we handle personal data, please contact Nicholas Standeven.

FAQ
What records should we retain?
Under the GDPR, data must be 'adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed'.

The GDPR applies to both electronic personal data and to manual filing systems where personal data are accessible according to specific criteria.

How long should we hold client data under the GDPR?

The GDPR does not set specific limits on data retention. It requires that the period for which personal data are stored is no longer than necessary for the task performed.

The minimum periods for which we shall retain working papers are as follows:

Type	Time frame
Accounts and Tax working papers	7 years from the end of the tax year, or accounting period, to which they relate
Files on clients or former clients' chargeable assets and gifts	8 years (then return them to the client or former client or obtain authority from the client or former client for their destruction)

Tax files and other papers that are legally the property of the client or former client shall be returned to the client (or former client) after each job is completed. If Crossley & Co are still in possession after seven years, authority should be obtained for their destruction.

When deciding how long to retain data, you should:

- consider legal retention period requirements;
- the period of time during which actions may be brought in the courts, and which records and working papers might be needed as evidence;
- the period of time for which information in the working papers might be required for use in compiling tax returns;
- the current and future use and relevance of the information;
- the costs, risks and liabilities associated with retaining it;
- the ease or difficulty of making sure it remains accurate and up to date;
- securely delete information that is no longer needed for this purpose or these purposes; update, archive or securely delete information if it goes out of date.

Ex-clients' records

There are no specific limits or guidance on this, but it may depend, in part, upon the lawful basis for processing that data and what is necessary (rather than just useful) for that purpose.

All client records must be returned to them upon cessation of our engagement.

For general data retention policies, we need to balance the requirement to only keep data for the minimum amount of time with their obligations to HMRC, clients etc.

Anti-money laundering rules require keeping records for five years after the relationship ends. Furthermore, the updated money laundering regulations (The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017) set out in Regulation 40 (5) that any personal information obtained for the purposes of the regulations must be deleted after five years from the end of a business relationship unless:

- the business is required to retain it under statutory obligation, or
- the business is required to retain it for legal proceedings, or
- the data subject has consented to the retention.

The ICO's data protection guidance acknowledges that it may not be necessary to delete all personal data when the relationship ends. Under the GDPR, individuals have a right to have personal data erased, known as the 'right to be forgotten'. This could apply where processing is no longer necessary for the purpose; where the data subject withdraws consent; if the individual objects to processing undertaken for legitimate interests; or where there are legal requirements to do so.

If a client leaves and asks for all personal information to be deleted, we should assess whether further retention is necessary and respond to the client within one month, explaining the next steps and rationale.

Delete data

ICO guidance states that 'The word 'deletion' can mean different things in relation to electronic data.

- There is a significant difference between deleting information so it cannot be retrieved and merely archiving data, which is not deletion and therefore still subject to the same data protection rules as 'live' data.
- There has to be a justification for retention more than 'just in case'.

What are the suggested secure ways to communicate personal data?

The ICO guidance indicates that 'The GDPR requires personal data to be processed in a manner that

- ensures its security,
- protects against unauthorised or unlawful processing and
- protects against accidental loss, destruction or damage.

The main ways in which Crossley & Co communicate to clients are set out below:

Portal: Unlike e-mail Iris OpenSpace is a secure document exchange facility. With the added benefit of allowing certain documents to be signed electronically. All files are encrypted in transit using SSL and AES technologies.

Emails: GDPR does not introduce a ban on the transfer of personal data or tax returns by email but there are risks in using this method. Permission must be obtained from the client prior to sending out documents via email, to ensure they are aware of the risks and happy to receive documents in this way. If requested, attachments sent via email, whether Excel or PDF, should be password protected. The password should be sent to the client in a separate email.

Dropbox: This is not used by Crossley & Co but some clients send files to us via Dropbox. The ICO suggests that the more sensitive the data, the less appropriate it will be to use 'off-the-shelf' cloud storage where the data controller is not in control of the terms and conditions.

What are the penalties for non-compliance with GDPR?

The administrative fines are discretionary rather than mandatory; they must be imposed on a case-by-case basis and must be 'effective, proportionate and dissuasive'.

There are two tiers of administrative fines that can be levied:
1) up to €10m, or 2% annual global turnover – whichever is higher.
2) up to €20m, or 4% annual global turnover – whichever is higher.