

General Data Protection Regulation (GDPR) Policy

1. Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

The goal of the data protection policy is to depict the legal data protection aspects in one summarising document. This will not only ensure compliance with the European General Data Protection Regulation (GDPR) but also to provide proof of compliance.

Further details on GDPR can be obtained from the Information Commissioner's Office (ICO)

2. Scope

This policy is relevant to all data the company holds and processes on behalf of others that is related to an identifiable individual.

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.

GDPR requires personal data to be:

- a) **processed lawfully**, fairly and in a transparent manner in relation to individuals;

Coverdale K9 has chosen the bases of legitimate Interest, legal obligation and contract for the lawful basis of processing the various data it deals with.

Coverdale K9 personal information collects and for each activity, the 'lawful basis' for doing so has been considered and documented in the line with the ICO's own guidance.

- 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;

Coverdale K9' revised *Privacy Policy* clearly explains that personal data collected will only be used for the purposes for which it is provided it to Coverdale K9, as indicated at the time the individual provided their personal data. It will also be used to administer, support and obtain feedback on the level of our services, to help prevent breaches of security, the law or our contract terms.

- c) **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed;

For each activity, we have considered the legitimate purpose for the information we have collected.

General Data Protection Regulation (GDPR) Policy

- 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;
- 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; and

Coverdale K9 has carefully considered how long it keeps information identifiable to the individual. Wherever possible, Coverdale K9 takes steps to keep identification to a minimum, particularly with regards to sensitive information.

- 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.

Coverdale K9 has implemented robust security processes to ensure that information is kept secure at all times and ensures that agreements are in place with all third party providers to ensure that information is kept safe and in line with Coverdale K9' expectations.

3. Responsibility

This policy applies to all Coverdale K9 staff, visitors and contractors and they are responsible for ensuring data is collected, stored and handled appropriately. This document was prepared by the Data Protection Officer of Coverdale K9 and approved by the Coverdale K9' Senior Management Team.

Each person that handles personal data must ensure that it is handled and processed in-line with this policy including any data protection principles. Responsibility and authority for specific activities are documented below.

Coverdale K9 also ensures that appropriate agreements are in places with those for whom Coverdale K9 processes data and for those who process data on Coverdale K9' behalf to ensure data is kept in accordance with the GDPR guidelines and the Data Protection Act 2018.

Directors

They have overall responsibility for ensuring that the organisation complies with its legal obligations.

General Data Protection Regulation (GDPR) Policy

Data Protection Officer

Their responsibilities include:

- Briefing the Senior Management on Data Protection responsibilities
- Reviewing Data Protection and related policies. This policy will be reviewed at least annually.
- Advising other staff on Data Protection issues
- Notification if requested by Senior Management
- Handling subject access requests

All Department Heads

Each department where personal data is handled should be, alongside the Data Protection Officer, responsible for drawing up its own operational procedures (including induction and training) to ensure that good Data Protection practice is established and followed.

The relevant senior competent member of staff must ensure that the Data Protection Officer is informed of any changes in their uses of personal data that might affect the organisation's notification process.

Staff

All staff should be required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work.

4. Confidentiality

Access in this case means not just by staff, but also by people outside the organisation and processors who handle personal information on behalf of Coverdale K9.

Normally access will be defined on a "need to know" basis; no one should have access to information unless it is relevant to their work. This may be relaxed in the case of information, which poses a low risk.

- The only people able to access data covered by this policy are those who need it for their work
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Guidance will be provided to all employees to help them understand their responsibility when handling data.
- Personal data should not be disclosed to unauthorised people, either within the company or externally.
- We ensure that robust contracts detailing Coverdale K9' expectations regarding data handling, data protection and data security are in place with those whom we contract with to handle personal information on our behalf.
- Employees should keep all data secure by taking sensible precautions and following the guidelines

General Data Protection Regulation (GDPR) Policy

5. Data Storage

The company has procedures for data storage and recovery on the computer system but when data is stored on paper it should be kept in a secure place where unauthorised people cannot gain access. Our data storage processes ensure:

- All unwanted personal data or printout must be shredded and disposed of securely.
- Data stored on removable devices must be kept locked away securely when not being used.
- Data is stored on designated drives and servers.
- Servers containing personal data are sited in a secure location.
- All servers and computers containing data are protected by approved security software.
- Data is stored at a secure level appropriate for the type of data.
- Data is stored in a format that allows the business to comply with subject access requests.
- Coverdale K9 ensures that robust contracts detailing Coverdale K9' expectations regarding data handling, data protection and data security are in place with those who we contract with to handle personal information on our behalf.

6. Basis for processing personal information

Coverdale K9 will only process personal data where we have a legal justification for doing so.

7. Special Categories of personal data

Sensitive personal information is also referred to as 'special categories of personal data' or 'sensitive personal data'. Coverdale K9 may from time to time need to process sensitive personal information. We will only process sensitive personal information if we have a lawful basis for doing e.g. it is necessary for the performance of the employment contract, to comply with the company's legal obligations or for the purposes of the company's legitimate interests.

8. Criminal records information

Certain conditions relate to the processing of criminal record information. Coverdale K9 does not currently process any criminal information data.

9. Privacy notice

The Company will issue privacy notices from time to time, explaining the type of personal information that we collect and hold, how this personal information is used and for what purposes.

Coverdale K9 will take appropriate measures to provide information in privacy notices in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

General Data Protection Regulation (GDPR) Policy

10. Accuracy

Coverdale K9 takes steps to ensure that the data is kept;

- Up to date
- Relevant for the its requirement
- Comply with the consent of the data subject
- Regularly reviewed

11. Retention periods

Personal data should not be retained for longer than is necessary for the purpose it was obtained for and in line with current standards and legislation.

12. Subject access request

All individuals who are the subject of personal data held by Coverdale K9 and processors working on our behalf are entitled to:

- Ask what information the company holds about them and why.
- Ask how to gain access to it.
- Be informed how to keep it up to date.
- Be informed how the company is meeting its data protection obligations.

13. Data breaches

A data breach may be one of the following:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams;
- blagging' offences, where information is obtained by deceiving the organisation which holds it.

Relevant personal data breaches must be reported (Notify) to the ICO within 72 hours of becoming aware of the breach, where feasible. If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without undue delay. Robust breach detection, investigation and internal reporting procedures are place. This facilitates decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals. A record of any personal data breach is kept. Details relating to breaches are logged here regardless of whether we are required to notify external authorities.

General Data Protection Regulation (GDPR) Policy

When a personal data breach has occurred, we must establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify the ICO; if it's unlikely then we don't have to report it. All breaches, actions and the decision of whether it is necessary to report to the ICO must be fully logged and documented.

14. Training

Coverdale K9 will ensure that staff are adequately trained regarding their data protection responsibilities. Individuals whose roles require regular access to personal information, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

Appendix 1 – Retention Periods

The main UK legislation regulating statutory retention periods is summarised below. If there is any doubt, non-health/medical records should be kept for at least 6 years, to cover the time limit for bringing any civil legal action.

Statutory records

Accident books, accident records/reports

Statutory retention period: 3 years from the date of the last entry (or, if the accident involves a child/ young adult, then until that person reaches the age of 21). (See below for accidents involving chemicals or asbestos).

Statutory authority: The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR) (SI 2013/1471) as amended, and Limitation Act 1980. Special rules apply concerning incidents involving hazardous substances (see below).

Accounting records

Statutory retention period: 3 years for private companies, 6 years for public limited companies.

Statutory authority: Section 221 of the Companies Act 1985 as modified by the Companies Acts 1989 and 2006.

Income tax and NI returns, income tax records and correspondence with HMRC

Statutory retention period: not less than 3 years after the end of the financial year to which they relate.

Statutory authority: The Income Tax (Employments) Regulations 1993 (SI 1993/744) as amended, for example by The Income Tax (Employments) (Amendment No. 6) Regulations 1996 (SI 1996/2631).

Medical records as specified by the Control of Substances Hazardous to Health Regulations (COSHH)

Statutory retention period: 40 years from the date of the last entry.

General Data Protection Regulation (GDPR) Policy

Statutory authority: The Control of Substances Hazardous to Health Regulations 1999 and 2002 (COSHH) (SIs 1999/437 and 2002/2677).

Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence

Statutory retention period: 3 years after the end of the tax year in which the maternity period ends.

Statutory authority: The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960) as amended.

Wage/salary records (also overtime, bonuses, expenses)

Statutory retention period: 6 years.

Statutory authority: Taxes Management Act 1970.

National minimum wage records

Statutory retention period: 3 years after the end of the pay reference period following the one that the records cover.

Statutory authority: National Minimum Wage Act 1998.

Records relating to working time

Statutory retention period: 2 years from date on which they were made.

Statutory authority: The Working Time Regulations 1998 (SI 1998/1833).

Non-statutory records

For many types of HR records, there is no definitive retention period: it is up to the employer to decide how long to keep them. Different organisations make widely differing decisions about the retention periods to adopt. An employer must consider what would be a necessary retention period for them, depending on the type of record.

Where the recommended retention period is 6 years, this is based on the 6-year time limit within which legal proceedings must be commenced under the Limitation Act 1980. So where documents may be relevant to a contractual claim, it's recommended that these are kept for at least the corresponding 6-year limitation period.

The GDPR legislation does not set out any specific minimum or maximum periods for retaining personal data. Instead, it says that:

'Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.'

Coverdale K9 is committed to ensuring that data collected is only stored for as long as it necessary and will continue to:

- review the length of time we keep personal data;
- consider the purpose or purposes we hold the information for in deciding whether (and for how long) to retain it;

General Data Protection Regulation (GDPR) Policy

- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.
- Undertake regular audits to ensure superfluous information is deleted securely and in a timely fashion.

Signed Suzanne Chappel

Dated 04/01/2020

Version 1