



Data Protection Policy / GDPR Compliant.

1. Purpose

This policy applies to the personal data of job applicants, employees, workers, contractors, volunteers, interns, apprentices and former employees, referred to as HR related personal data. This policy does not apply to the personal data of clients or other personal data processed for business purposes.

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998 and, in substitution from 25 May 2018, the General Data Protection Regulation 2018 (“GDPR”) in respect of handling and processing personal data.

It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically. All staff involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines.

2. Definition of Personal Information / Data?

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

3. Data Protection Principles

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

- Personal data shall be processed fairly and lawfully.
- Personal data shall be obtained only for one or more specified and lawful Purposes.
- Personal data shall be adequate, relevant and not excessive.
- Personal data shall be accurate and where necessary, kept up to date.
- Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes.
- Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998.
- Personal data shall be kept secure i.e. protected by an appropriate degree of security.

- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

4. Compliance with data protection principles

Cano Training Services does not use the data for any other purpose and it reviews its processing and policies regularly to ensure that it is not using special category personal data or criminal records data for any other purpose. The organisation will not do anything unlawful with personal data. Special category personal data and criminal records data are not disclosed to third parties, except in the context of seeking medical advice from the organisation's occupational health adviser or other medical advisers who are subject to a professional duty of confidentiality. As far as possible, information required for equal opportunities monitoring purposes is kept in an anonymised form. Monitoring forms are kept under review to ensure that the information collected is accurate and not excessive.

Criminal records checks are carried out only for individuals undertaking roles where the organisation is under a legal obligation or regulatory requirement to perform such checks. Cano Training Services keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay. We take reasonable steps to ensure that the personal data that it holds is accurate. Special category personal data and criminal records data is obtained:

- directly from job applicants, employees and other data subjects; or
- from external sources that the organisation is entitled to assume will provide accurate information, such as the Disclosure and Barring Service in the case of criminal records data, or medical professionals in the case of health data.

5. Individual Rights

Individuals have a number of rights in relation to their personal data. Subject access requests Individuals have the right to make a subject access request. If an individual makes a subject access request, Cano Training Services will tell them:

- whether or not their data is processed and if so why, the categories of personal data concerned and the source of the data if it is not collected from the individual;
- to whom their data is or may be disclosed, including to recipients located outside the European Economic Area (EEA) and the safeguards that apply to such transfers;
- for how long their personal data is stored (or how that period is decided);
- their rights to rectification or erasure of data, or to restrict or object to processing;
- their right to complain to the Information Commissioner if they think the organisation has failed to comply with their data protection rights; and

- whether or not the organisation carries out automated decision-making and the logic involved in any such decision-making. We will also provide the individual with a copy of the personal data undergoing processing. This will normally be in electronic form if the individual has made a request electronically, unless they agree otherwise.

To make a subject access request, the individual should send the request to becky@canotrainingltd.com. In some cases, Cano Training Services may need to ask for proof of identification before the request can be processed. We will inform the individual if it needs to verify their identity and the documents it requires.

5.1 Other rights

Individuals have a number of other rights in relation to their personal data. They can require the organisation to:

- rectify inaccurate data;
- stop processing or erase data that is no longer necessary for the purposes of processing;
- stop processing or erase data if the individual's interests override the organisation's legitimate grounds for processing data (where the organisation relies on its legitimate interests as a reason for processing data);
- stop processing or erase data if processing is unlawful; and
- stop processing data for a period if data is inaccurate or if there is a dispute about whether or not the individual's interests override the organisation's legitimate grounds for processing data. To ask Cano Training Services to take any of these steps, the individual should send the request to becky@canotrainingltd.com.

6. Data Security

The organisation takes the security of HR-related personal data seriously. Cano Training Services has internal policies and controls in place to protect personal data against loss, accidental destruction, misuse or disclosure, and to ensure that data is not accessed, except by employees in the proper performance of their duties. Where Cano Training Services engages third parties to process personal data on its behalf, such parties do so on the basis of written instructions, are under a duty of confidentiality and are obliged to implement appropriate technical and organisational measures to ensure the security of data.

6.1 Data security could include:

- Install a firewall and virus-checking on your computers.

- Make sure that your operating system is set up to receive automatic updates.
- Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.
- Only allow your staff access to the information they need to do their job and don't let them share passwords.
- Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.
- Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don't lose the information.
- Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).
- If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.
- Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.
- If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient's arrangements are secure enough before sending your message.

7. Data breaches

If Cano Training Services discovers that there has been a breach of HR-related personal data that poses a risk to the rights and freedoms of individuals, it will report it to the Information Commissioner within 72 hours of discovery. The organisation will record all data breaches regardless of their effect. If the breach is likely to result in a high risk to the rights and freedoms of individuals, it will tell affected individuals that there has been a breach and provide them with information about its likely consequences and the mitigation measures it has taken

8. Individual Responsibilities

Individuals are responsible for helping the organisation keep their personal data up to date. Individuals should let the organisation know if data provided to the organisation changes, for example if an individual moves house or changes bank details.

Individuals may have access to the personal data of other individuals and of our customers and clients in the course of their employment, contract, volunteer period, internship or apprenticeship. Where this is the case, Cano Training Services relies

on individuals to help meet its data protection obligations to staff and to customers and clients. Individuals who have access to personal data are required:

- to access only data that they have authority to access and only for authorised purposes; • not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation; • to keep data secure (for example by complying with rules on access to premises, computer access, including password protection, and secure file storage and destruction); • not to remove personal data, or devices containing or that can be used to access personal data, from the organisation's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes; and
- to report data breaches of which they become aware to the data protection officer immediately. Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the organisation's disciplinary procedure. Significant or deliberate breaches of this policy, such as accessing employee or customer data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

9. The General Data Protection Regulation 2018

Cano Training Services has adapted its policies and procedures to ensure it is compliant with the GDPR. This will be reviewed annually and updated as processes are developed.

Under the GDPR, individuals have certain rights when it comes to the control of personal data:

1. The right to be informed. Individuals have the right to be given information about how their data is being processed and why. Cano Training Services has provided this policy to show how we handle your data.

2. The right of access. Cano Training Services has a duty to comply with the requirements of Subject Access Requests (SAR)

3. The right to rectification. The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete.

4. The right to be forgotten. You have the right to ask Cano Training Services to remove your data.

5. The right to restrict processing. You may restrict processing for a legitimate reason, we would still have the right to hold that information.

6. The right to data portability. You may be able to obtain the information we hold about you and use it for your own purposes. Conditions apply.

Should you wish to exercise any of your rights above, please email becky@canotrainingltd.com stating the following information:

Your Name, Your Contact details, Your Relationship to Subject, Full details of information relating to your request, Reason for request and the right being

exercised. You will be asked to verify your identity if you are the subject, alternatively you will be asked to provide consent from the subject if you are a representative. Should we require further information we will contact you. Your request will be dealt with within 1 month of receipt of your request.

Revised Date: October 2021
Rebecca Cano-Lopez
Company Director
Cano Training Services Ltd