Ecordia - Data Protection Policy (2018)
- for implementation in May 2018.

ICO Registered: ICO. Z1791567

Why this policy exists

This data protection policy ensures Ecordia:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers, partners and Ecordia users
- Is open about how we store and process individuals' data
- Protect ourselves from the risks of a data breach

Roles

- Ecordia is a data processor (data storage/system provider).
- Training providers, assessment centres and Colleges are data controllers and processors.

Data protection law

The Data Protection Act 1998 describes how organisations — including Ecordia — must collect, handle and store personal information.

These rules apply regardless of whether data is stored electronically, on paper or on other materials.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

The Data Protection Act is underpinned by eight important principles. These say that personal data must:

1. Be processed fairly and lawfully
2. Be obtained only for specific, lawful purposes
3. Be adequate, relevant and not excessive
4. Be accurate and kept up to date
5. Not be held for any longer than necessary
6. Processed in accordance with the rights of data subjects
7. Be protected in appropriate ways
8. Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Stored Data

- The data controllers (training providers, assessment centres and Colleges) will need to store some personal data (staff and learners) on the Ecordia system.
- The amount of personal data stored on Ecordia is entirely at the discretion of the training provider and can include information such as name, postal address, email address, date of birth, telephone numbers and national insurance number.
- Data is only processed and stored via the Ecordia web application. Ecordia does not store or process data in any other way except for communications from customers and users for system support reasons that may contain names, email addresses and telephone numbers. This data is deleted after three years.

Security & Data Protection

- Is the Ecordia system secure?

  Ecordia is a SSL certified online application which is accessed over secure HTTPS protocol with 128-bit encryption.

  Regular testing of the effectiveness of security measures is undertaken. As a data storage provider and processor, we are required to notify the relevant controller of any breach without undue delay after becoming aware of it.

  All links to the Ecordia system are secure and inaccessible without encrypted authentication. Users are given an individual username and password to access the system. Users can only see the information they are responsible for.

  Training providers, assessment centres and FE Colleges should be aware that Ecordia is not liable for data breaches due to users not keeping their login information, session or IT systems secure.

- Where is data stored?

  The Ecordia system runs on the highest specification database, security and web servers hosted in EU-based Microsoft data centres– for improved performance, security, reliability and redundancy.

  These data centres are provided and serviced by the industry-leading Microsoft Azure web services, which have extremely high levels of network firewall protection, building security, surveillance and fire protection. These comply with EU-US Privacy Shield and EU Model Clauses.

  Customer and user files and documents are stored on Amazon AWS (S3) cloud storage service (within the EU) in a secure bucket which is not publicly accessible. Documents can only be accessed via the Ecordia application which stores unique encrypted keys for each document. These keys expire every 6 months and are renewed only via the Ecordia application on demand. Documents are deleted from S3 at the same time customer information is deleted from the Ecordia application.

- Data Retention

  Ecordia retains data for up to 7 years depending on assessment centre requirements - and in-line with industry guidelines. Centres can delete data sooner if required. Data will be deleted within 12 months at contract end points.

  It is recommended that training centres and learners/students archive work portfolios to their own computers or CD / USB memory stick for archive after course completion. Responsibility for the exported portfolios (which also contains user data) lies with the assessment centre as the data controller and data processor and not with Ecordia.

Data Processing & Access

- Ecordia only stores personal data to the extent authorised by the centres/controllers.
- Some aspects of user/customer data will be accessed to help support our users/customers, for example if an assessor has a query specific to a certain portfolio, then our Support Team will need to access their data / portfolios. Statistics such as achievement rates may also be analysed for general Ecordia statistical purposes only.
- Assessment centre specific data and information will never be disclosed to third parties without prior written agreement.
- Controller's written permission will be sought before engaging with any sub-processors.
- An Ecordia Data Protection Officer has been appointed.
- All Ecordia staff have been notified of recent updates to our data protection policy and have received training on data security and GDPR.

Consent To Store Data

- On first login, all users and learners are asked for consent for storing personal data, such as name, address, email address, date of birth, national insurance number, to be held on Ecordia and accessed by parties, people and organisations involved their qualification/course, such as the assessment centre, training provider, College and workplace.

Data Controllers & Processors

Ecordia customers, training providers, assessment centres and Colleges should all be aware that by using Ecordia to manage and deliver training and assessments, they are the data controllers and processors and have the following responsibilities to their staff, learners and other users under their Ecordia centre account:

- Rights of access
- Right to rectification and data quality
- Right to restrict processing
- Right to erasure including retention and disposal

As the data controller, it is the assessment centre's responsibility to restrict access/provide access or delete the candidate portfolio should they wish to, prior to the 7-year point where portfolio data will be automatically deleted.

- Right of access – the Ecordia system has functionality to enable data controllers to respond to individuals' requests for access to their personal information.
- Right to rectification and data quality - the Ecordia system has functionality to enable data controllers to edit personal data held on the system so that it remains accurate and up-to-date.
- Right to erasure – the Ecordia system has functionality for data controllers to securely dispose of personal data that is no longer required. Ecordia also has processes to routinely and securely dispose of personal data that is no longer required or is beyond the time limit specified with the data controller (maximum of 7 years).
- Right to restrict processing – the Ecordia system has functionality to enable data controllers to suppress processing of specific data.
- Right of data portability – the Ecordia system has functionality for the data controller to supply the personal data we process in electronic format (exported portfolio).

Please communicate with Ecordia if you require any assistance with the above.

Online Privacy Policy

- Ecordia's privacy policy has been updated in-line with GPDR guidelines and is accessible to all customers and users. http://www.ecordia.co.uk/privacy-statement