Agylia Learning Management System

GDPR FAQ

www.agylia.com

Version 1.0

What is GDPR?

The European Union **General Data Protection Regulation** (GDPR) will potentially repeal and replace the Data Protection Act 1998. It applies uniformly across EU member states. It is technology neutral but has better safeguards in comparison to the Data Protection Act it will replace, to reflect 'real world' data processing.

The Data Protection Act is no longer fit for purpose because it was drafted prior to the exponential growth of the Internet. Personal data is now being used in ways that were not envisaged at the time.

When does GDPR come into force?

GDPR becomes applicable on **May 25th 2018**, exactly two years after a formal 'transition period' came into force.

How will 'Brexit' affect GDPR and Agylia's GDPR obligations?

Once the United Kingdom has left the European Union, GDPR regulations will still apply because any non-EU business will be subject to GDPR if they offer goods or services to EU residents.

Agylia are committed to upholding and applying GDPR even after the UK leaves the European Union. Agylia are currently monitoring the Brexit situation, in case any obligations were to change.

What are Agylia's obligation's in relation to GDPR?

Agylia is a **data processor** as defined by GDPR i.e. the Agylia platform stores and processes personal data, on behalf of, and with the consent of the **data controller**. The Agylia customer will upload personal data (of their choosing) for their users of the platform (learners and administrators).

As a data processor, Agylia's obligations under GDPR are to:

- Act ONLY under the instructions of the data controller (Agylia customers)
- Keep personal data secure from unauthorised access, loss or destruction

Why does Agylia need to store and process any personal data?

Strictly, Agylia does not need to store and process personal data and all user data loaded onto the platform could be anonymised. However, in practice, a digital learning platform such as Agylia needs to be able to identify users and track learning activity so that it can provide a sensible set of reporting data to the customer's system's administrators and reporters.

While Agylia will take every precaution to ensure that customer's personal data remains secure, the onus is on the customer to minimise the set of personal data uploaded to the platform i.e. restrict it to the 'necessary' set and no more. This is referred to as the '**data minimisation principle'**.

What personal data does Agylia store and process?

As a data processor, Agylia stores and processes personal data relating to people who access the Agylia platform. This includes customer admins and customer end users (learners). The precise type of personal data maintained depends on the specific

T +44 (0) 1454 269222 E info@agylia.com **www.agylia.com**

Agylia, Tortworth House, Wotton-under-Edge, Gloucestershire, GL12 8HQ. Registered in England, no. 3863494.

customer implementation and the data that the customer would like to maintain for their user population for example for reporting purposes.

Typically, due to usability and reporting requirements, personal data includes **email addresses**, **first names** and **surnames**. In addition, details relating to a user's job role, department, location and so on are often stored, but this is entirely based on the user profile fields specified by the customer at system implementation time.

Does Agylia store sensitive personal data?

No. *Sensitive personal data* (as defined by GDPR) for example that relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, physical or mental health records, sex life or sexual orientation, genetic or biometric data are **not** stored by the platform.

How does Agylia adhere to the obligations of GDPR?

Agylia takes every reasonable precaution to protect customer's personal data. This includes appropriate technical and organisational measures. Agylia adheres to the eight data protection principles as defined by Article 5 of GDPR. These are:

The lawfulness, fairness and transparency principle
Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (as outlined in the platform's privacy notices visible to all data subjects)

The purpose limitation principle
Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

The data minimisation principle
Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The accuracy principle
Personal data shall be accurate and, where necessary, kept up to date.

The storage limitation principle
Personal data shall be 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. Agylia deletes personal data at the request of the data controller.

The integrity and confidentiality principle
Personal data shall be 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.

Does Agylia transfer personal data across boarders?

No. Personal data is not transferred across borders. Agylia customers' personal data is stored on servers either in the European Union or the United States of America. Data is not transferred between the two.

What happens in the event of a data breach?

T +44 (0) 1454 269222 E info@agylia.com **www.agylia.com**

Agylia, Tortworth House, Wotton-under-Edge, Gloucestershire, GL12 8HQ. Registered in England, no. 3863494.

GDPR defines a personal data breach as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted or otherwise processed.

In the event of a data breach, Agylia invokes its Data Breach Policy. This is defined in the Agylia policy document "*ISMS Doc 16.1a – Agylia Data Breach Policy*" maintained within Agylia's Information Security Management System (ISMS) as part of their ISO 27001 commitments. A copy of this policy document is available on request.

GDPR Terminology

To understand GDPR you need at least a basic understanding of the core terminology.

- **Data subject**
  A **data subject** is an individual who is the subject of personal data. This does not include deceased individuals or an individual who cannot be identified or distinguished from others. Examples include employee, customer, consumer.

- **Data controller**
  A **data controller** is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

- **Data processor**
  A **data processor** is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- **Processing**
  In relation to information or data, **processing** means obtaining, recording or holding information of data, or carrying out any operation or set of operations on the information or data.

- **Personal data**
  The definition has subtly changed with the introduction of GDPR.

  According to the **Data Protection Act 1998**, personal data is:

  Data which relates to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

  According to GDPR, 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 **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.*

- **Sensitive personal data**

T +44 (0) 1454 269222 E info@agylia.com **www.agylia.com**

Agylia, Tortworth House, Wotton-under-Edge, Gloucestershire, GL12 8HQ. Registered in England, no. 3863494.

Sensitive personal data is the term used by GDPR to represent a special category or personal data. Sensitive personal data is:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Physical or mental health records
- Sex life or sexual orientation
- Genetic data
- Biometric data

Please note that this guide is for information purposes only, and should not be relied upon as legal advice. We encourage you to work with legal and other professional counsel to determine precisely how GDPR might apply to your organisation.

T +44 (0) 1454 269222 E info@agylia.com **www.agylia.com**

Agylia, Tortworth House, Wotton-under-Edge, Gloucestershire, GL12 8HQ. Registered in England, no. 3863494.