GDPR Supplier Statement

Executive Summary

Grey Matter Learning (GML) is aware of the General Data Protection Regulation (GDPR) which came into effect on May 25th 2018. The regulations encompass a much wider and more robust set of rules and controls to ensure that subjects' data is protected appropriately, and includes data that we process on behalf of you, or your employees. We welcome these changes.

As data processors and data controllers, we are aware of our obligations to comply with the new regulations. We have adapted our policies, processes and other controls where we have identified that changes are required for GDPR. GML will maintain an active role in staying up-to-date with changes where the regulations are not yet clear or remain to be clarified through case law, and will update our own policies, processes and controls as required to deliver compliance for all of our Customers.

To achieve this, we are working with trainers, learning content specialists, intrusion and attack specialists, data protection specialists and legal experts to:

- Audit our GDPR preparations
- Prepare all of our staff with GDPR awareness training
- Update our contacts, contracts and service agreements
- Improve the rights of data subjects to control their own data
- Improve process controls for data destruction and deletion
- Implement mandatory notifications for data breaches
- Improve transparency and fair processing alerts and notifications
- Improve and amend privacy policies
- Seek consent where required

The remainder of this document describes in detail how GML will deliver its responsibilities under GDPR as your supplier of products and services.

Introduction

Grey Matter Learning (GML, us, we, our) processes data on behalf of individuals and organisations (Customers, clients, you) within the EU. GML also processes data on behalf of Customers outside of the EU. The information contained in this GDPR Supplier Statement (the Statement) describes how we ensure that we protect these data in compliance with the GDPR.

Data Collection, Obligations and Purpose

The Customer will determine the purpose and means of GML's processing of Customer personal data and provide instructions to GML to process Customer personal data in accordance with this purpose.

GML will process Customer personal data only for the purpose of providing, supporting and improving GML's products and services (including the provision of insights, learning and compliance reporting and other reporting), using effective and appropriate technical and organisational protective security methods and measures.

GML will not use Customer personal data for any other purpose.

GML will inform the Customer promptly if, in our opinion, an instruction from a Customer violates the GDPR and other applicable data protection requirements.

GML will take reasonable steps to ensure that persons employed by GML and persons engaged on our behalf comply with the terms of this statement.

GML will ensure that its employees, subprocessors and other agents engaged on our behalf will respect the confidentiality of Customer personal data and comply with the terms of this statement even after the end of their employment, engagement or contract.

GML will provide reasonable support and assistance to Customers regarding requests from data subjects for access to, rectification, erasure, restriction, portability, blocking or deletion of Customer personal data that GML processes on behalf of Customers.

GML will investigate personal data breaches and notify the supervisory authority and Customer data subjects.

GML will prepare data protection impact assessments (DPIA) where appropriate and necessary in consultation with the supervisory authority.

Some of our products and services process compliance data to provide evidence of staff safety to practise roles and responsibilities under the requirement of the Care Act 2014 and Care Certificate Standards.

GML processes the following personal data:

Product	**Personal Data**	**Reason For Processing**
Assessment, eLearning and competence recording	Name	To personalise learning experiences and correctly address the data subject.
	Email address	To enable email notification of trigger events occurring and to support certain essential features such as password reset.
	Service delivery site	To identify the location in which a specific role is practised (see job title below).
	Job title	To identify and address the role holder correctly and to differentiate the requirements to practice that role safely.

	System username	To provide a unique identification reference for each user.
	Evidence record	To provide a continuous record of role-related content including reflective practice, research, supervision input, etc. to evidence competence in performing that role.
	Observation record	To provide a record of role-related observations of practice to support decisions of competence.
Customer organisation profile	Organisation Name	To correctly identify Customer organisations.
	Details of key contacts	To manage Customer accounts effectively.
	Name	To personalise learning experiences and correctly address the data subject.
	Job title	To identify and address the role holder correctly and to differentiate the access requirements for that role.
	Email address	To enable email notification of trigger events occurring and to support certain essential features such as password reset.
	Telephone numbers	To correctly address people requesting service or support requests.
	Business address	To enable account management activities, such as billing and visits to a Customer premises to deliver training.
	Service delivery address	To correctly address the location where services are delivered as these will impact on how 'safety to practice' is understood.
Customer Relationship Management (CRM)	Name	To correctly address people requesting service or support requests.
	Email address	To correctly address people requesting service or support requests.

	Telephone contact number	To correctly address people requesting service or support requests.
	Organisation they work for	To ensure that contractual and service level agreement data is taken into proper consideration in supporting Customer requests for service or support.
Finance	Business Address	To address the invoice correctly to the business.
	Contact name	To direct emails to a named contact from our finance systems.
	Email address	To automatically send emails from our finance systems.
	Bank details (refunded monies)	To correct an overpaid or incorrectly paid invoice in instances where we provide a refund.

This data is processed in order to provide our products and services to Customers.

In the case of our online learning, assessment and competence recording products, this data is essential to many features of these products so that Customers can record and report on evidence of competence and safety to practice.

In the case of our facilitated learning courses, we use personal data to organise and communicate with delegates about courses.

All Customers have the option to consent to receive information from GML on products and services.

GML does not process special category data. We actively encourage Customers through training, contextual text and instructional text against adding any special category data or personal identifying information about, for example, the recipients of care in their evidence portfolio and will provide tools to obfuscate and otherwise anonymise data that is entered by Customers in free-text fields.

Governance

GML has a Data Protection Officer. The Data Protection Officer reports to the Managing Director.

The Data Protection Officer ensures that GML's commercial and operational activities are delivered in compliance with the prevailing data protection regulations in our jurisdiction. This role monitors and reports compliance, represents Customers, handles communication and coordinates all GML data protection activity.

GML will continue to have a data protection role in place for the foreseeable future.

GML has a robust Third Party Data Processing Agreement between data controllers and processors so that data is protected appropriately and adequately within the definitions of the regulations.

As part of our GDPR preparations, GML has built a central record of all processing activities which we are able to share with data controllers on request.

Storage and Archiving
GML stores personal information data on Third Party processors, who are contracted as subprocessors; see section on 'Using Subprocessors' for more information. This data is held off-site from GML in data centres. The data centres are in secure locations and access to data is secured according to roles within those organisations.

Personal information is also stored in temporary files on servers during the process of bulk-importing some new accounts, for example, where a Customer migrates their organisational accounts from another service provider. This data is destroyed as part of the import process on completion of the import.

GML processes are in place to centralise storage of all data in tightly defined secure digital systems and processes. Very few manual processes exist. Where manual processes do exist, these have been mapped and safeguards implemented to control the storage and access to this data. Overarching principles are in place to drive digitisation and safe destruction of manual records, with the resultant digital records processed in line with GDPR and the Customer contract.

A small number of documents such as paper invoices are kept in secure manual files in our office. We regularly digitise these documents to enable them to be processed, for example by uploading them to our secure finance systems, and then securely destroy the originals. Paper records awaiting digitisation remain locked in secure filing cabinets inside our access-controlled office building.

GML does not process sensitive personal data on behalf of a data controller.

Archived data is stored in an encrypted state using 256-bit Advanced Encryption Standard (AES-256)

Data is stored in data centres, in London and Farnborough, UK. It is stored on server hard disk drives and in backup images also stored in the data centre. Data is sent to an archive facility, which is encrypted and held privately.

Security
Physical access to GML offices is monitored by a GML duty staff member at all times and visitors are required to sign in on each occasion. Access to data within the office environment is tightly controlled and GML operates a "leave me, lock me" policy for all data (including technical resources). Any physical printouts of data are processed immediately and subsequently scanned and shredded.

Access to our sub-processor data centres is physically and functionally secured according to the principles established under ISO 27001. For example, access to data centres are regularly reviewed, audited, monitored and logged. Physical access is limited through CCTV and intrusion detection systems.

Administrative and technical roles are defined within GML and data requirements mapped to them. GML staff only have access to data enabled according to their role. For example access to Customer financial details is restricted to the Sales and Finance roles.

All GML staff have role-based access to our Customer Relationship Management (CRM) solution in order to deliver and maintain products and services for Customers.

External Customers can view their own or their organisation's compliance evidence data depending on their access rights in order to report on compliance against the prevailing regulatory framework for the sector, for example The Care Act and Care Certificate.

GML is authorised to process Customer personal data via contract. We will be renewing consent as appropriate to the GDPR.

We have a range of border and protective security devices and services in operation, including firewalls and encrypted network tunnels to deal with prevention of data breaches. We are currently working towards Cyber Essentials accreditation that ensures our systems have features in place to detect any breaches. We have an account creation policy with logs of the activity on that account. We also have intrusion detection software to detect potential breaches. We run network monitoring software to ensure that all traffic is coming from bonafide sources. We also have defined internal roles that outlines staff access to data. We have automated backups of systems to ensure the security and integrity of the data we process on behalf of controllers.

On detection of a data breach or intrusion, the relevant supervisory authority is notified of the activity within 72 hours of discovery. If the breach is deemed to affect the rights and freedoms of individuals, GML will ensure all affected parties are informed.

GML will follow the steps outlined in our Incident Management policy and process. A record is made of the breach which can be made available at the request of the ICO or other appropriate supervisory authority.

Data held internally is access-controlled and only available to staff with specific access needs in order to deliver contracted services on behalf of a Customer. All access to data is logged and routinely reviewed for inappropriate access.

Our Service Management policy (May 2018) contains an updated subsection for 'security incident management' which covers data breach incidents. Our Security Incident Management process (May 2018) contains mandatory notification to the ICO within 72 hours of discovery of a breach.

The Security Incident Management process also includes mandatory notification for data controllers, where GML acts as a data processor, as appropriate on detection of a breach, and within 24 hours.

Destruction of Data and Termination of Contract
GML takes its responsibility for destruction of data seriously and executes data destruction in accordance to the standards outlined in ISO 27001.

We follow best practice when deleting data to reduce the risk of leaking that information to a third party. Initially, disks and SSDs are overwritten with dummy data to prevent soft-delete, and then are reclaimed for further use. When hardware is deemed fit for retirement, it is disposed of using secure destruction techniques that include overwriting data followed by physical destruction of the storage media so that data cannot be restored or reconstructed following the destruction process.

Authorisation of destruction will be given by the IT Director. We hold an agreement with Amazon Web Services in relation to their data retention and deletion policies. Ultimately, GML will initiate data destruction within 90 days of the contract termination.

Using Subprocessors
We have contracts in place with Amazon Web Services and Buckhill who provide hosting and processing for our services. We use Amazon's London, UK data centre to host websites and learning materials. Our hosting services including eLearning and website services are hosted with Buckhill in a data centre in Farnborough, Hampshire, UK.

GML uses subprocessors such as Amazon AWS and Buckhill to host our products. All of our subprocessors and the activities they undertake to process data securely are within the EEA. All subprocessors are required to demonstrate robust compliance with GDPR and other protective security requirements. As your data processor, GML will inform you, the controller, of any intended changes concerning the addition or replacement of other subprocessors not included here.

GML has written agreements in place covering our subprocessor arrangements. We require that our subprocessors are similarly compliant with the GDPR as a condition of use.

We expect our subprocessors to employ the protective security standards outlined in the GDPR and ISO 270001 where personal data is held on our servers.

Amazon is reliant on their own hardware and ISO 27001 certified data centres. Buckhill uses ISO 27001 certified subprocessors Datum and Wanstor for their data centre and business continuity and storage services. At the time of this document version, all of our subprocessors and their subprocessors are GDPR compliant.

Transfers of Personal Data
Internal Data flows within GML are closely monitored and access is granted according to the roles and responsibilities discussed in Security.

No data is shared with Third Parties outside of the organisation without specific consent from the data owner. Where data is transferred to Third Parties, this is done securely via encrypted Open API connections to deliver specific functionality to Customers, including HR, language translation, resource scheduling and other Enterprise Resource Planning (ERP) platforms in order to meet the requirements of a Customer contract; for example, to provide learning evidence data to enable competent staff to be scheduled for front-line care activities. Where GML shares data with Third Parties in this way, we ensure that our partners employ appropriate protective security measures and are themselves compliant with GDPR.

Where data is transferred within GML, this is completed via our secure services using TLS/SSL connections between internal platforms with individual access rights granted according to a principle of minimum access. Physical data storage is minimised and full control is maintained and auditable.

GML has facilities to send and receive public/private key encrypted email where necessary. We also provide secure tools and methods for Customers to add and retrieve personal data via encrypted TLS/SSL connections to our application architecture. Data transferred within our systems is appropriately connected via secure technologies including protocols, boundary devices, monitoring services, intrusion detection services and also via policies and processes governing the appropriate handling of processed data.

GML exclusively processes data within the EEA. We primarily serve Customers in the UK and Europe and disclose data to people and organisations within the EEA. Our staff are based within the EEA.

Occasionally a Customer will access our systems from a location outside of the EEA; for example, where a manager views compliance reports while away from the UK. In these instances, only the data to which the manager has access are disclosed according to their access privileges. This data is additionally protected in transit via SSL/TLS technologies. Client access is granted via secure sessions which time out after a short period of inactivity.

GML exclusively processes data within the EEA.

Training

All GML team members have undertaken GDPR training in the form of eLearning. This activity was part of our GDPR preparations and coordinated by our project team. We also held team briefings and involved all staff in specific pieces of GDPR work to ensure there is understanding, engagement and accountability.

Refresher training will be planned at an appropriate point in time, dependent on the individual's role and responsibilities. This will be led by the Data Protection Officer.
Our team have been made aware that unlawful access to data and/or disclosure of personal data is prohibited through training, briefings and discussions. We will be amending contracts of employment and consulting with our team about this amendment to further embed this legislation into our company's culture.

All of our team, including The Board, Senior Management, the security and IT team, our Service Desk and all other staff have been involved in GDPR awareness sessions.

Responding to Requests for Access to Subject Data

GML provides tools and methods for Customers to access their personal data while using our product ecosystem. GML will further support Customers and provide access to Customer data on reasonable request or on termination of data processing services. GML will make all Customer personal data available to the Customer and securely destroy all copies of these personal data in line with our data destruction policy, unless data protection requirements or overarching lawful reasons prevent GML from making this data available and destroying all or part of the Customer personal data disclosed. Where this happens, GML will preserve the confidentiality of Customer personal data and will only actively process such data to comply with applicable laws.

Where GML acts as data processor, we will respond to requests from data controllers promptly.

Where GML receives requests for access to subject data directly from a data subject, we will refer the request to the data controller for response promptly, and within three working days of receipt of the request.

Where GML receives a request for access to subject data from any person or party which suggests non-compliance with current data protection legislation, we will immediately inform the data controller and not enter into further communication with the requesting person or party unless expressly authorised to do so by the data controller.