

Data Processing Agreement (DPA)

This Data Processing Agreement ("DPA") sets out the rules governing the processing by 2BITS of personal data entrusted by the Customer in connection with the provision of MyLearningDay services.

1. Application of the DPA

The DPA applies where, in the course of providing the Services, 2BITS processes personal data on behalf of the Customer. To that extent, the Customer is the data controller and 2BITS is the processor.

The DPA forms part of the Agreement entered into between the Customer and 2BITS. Capitalised terms not defined in the DPA have the meanings given to them in the Terms of Service or the EULA.

The DPA does not apply to personal data processed by 2BITS as an independent data controller. The rules governing such processing are described in the Privacy Policy.

2. Subject Matter and Scope of Processing

2BITS processes personal data to the extent necessary to make available, maintain, secure and support the Platform and to perform the other Services specified in the Agreement.

Processing takes place for the term of the Agreement and for the period technically necessary to return or delete the personal data, taking into account the backup retention cycle and obligations arising under applicable law.

The subject matter, nature, purpose and scope of processing, as well as the categories of data subjects and personal data, are specified in Annex 1.

3. Customer Instructions

2BITS processes personal data only on the Customer's documented instructions, unless processing is required by European Union or Member State law. 2BITS will inform the Customer of such a legal requirement before processing begins, unless the law prohibits such information from being provided.

Documented instructions include, in particular, the provisions of the Agreement, the configuration of the Platform, actions of the Customer's authorised administrators, requests submitted to support and other instructions provided in documentary form.

If, in the opinion of 2BITS, a Customer instruction infringes data protection laws, 2BITS will inform the Customer and may suspend performance of the instruction until the matter has been clarified.

Personal data is transferred outside the European Economic Area only on the Customer's instructions or to the extent necessary to perform the Agreement and on the basis of a mechanism permitted under data protection laws.

4. Obligations of 2BITS

2BITS:

- processes personal data only on the Customer's documented instructions in accordance with Section 3 of the DPA;
- ensures that persons authorised to process personal data have committed themselves to confidentiality or are subject to an appropriate statutory obligation of secrecy;
- restricts access to personal data to persons who require it to perform their duties;
- engages sub-processors in accordance with Section 6 of the DPA;
- is required to return or delete personal data in accordance with Section 10 of the DPA;
- implements appropriate technical and organisational measures, as described in Annex 2;
- maintains processing records required by law;
- does not use the entrusted personal data for its own marketing purposes or to create independent profiles of Users;
- makes available to the Customer the information necessary to demonstrate compliance with the obligations arising under Articles 28 and 32–36 of the GDPR.

5. Obligations of the Customer

The Customer is responsible for the lawfulness of personal data processing, in particular for:

- determining the purposes and legal bases of processing;
- fulfilling information obligations;
- ensuring that instructions given to 2BITS comply with applicable law;
- the scope of personal data entered into the Platform;
- managing accounts, permissions and data retention to the extent supported by the Platform;
- handling data subject requests and assessing obligations related to personal data breaches.

The Customer should not enter special categories of personal data or personal data relating to criminal convictions and offences into the Platform unless doing so is lawful, necessary and subject to appropriate safeguards.

6. Sub-processors

The Customer grants 2BITS general authorisation to engage sub-processors to the extent necessary to provide the Services.

2BITS requires each sub-processor to protect personal data on terms providing at least the same level of protection as that required under the DPA. 2BITS remains liable to the Customer for the performance of those obligations to the extent required by law.

2BITS makes the current list of sub-processors available to the Customer. 2BITS will provide the Customer with reasonable advance notice of any intended addition or replacement of a sub-processor.

The Customer may raise a reasoned objection on data protection grounds. The Parties will then attempt to agree on a reasonable solution. If no such solution can be reached, the rules governing amendment or termination of the Agreement apply.

7. Assistance to the Customer

Taking into account the nature of processing and the information available, 2BITS assists the Customer, to the extent required by the GDPR:

- in responding to data subject requests;
- in ensuring the security of processing;
- in assessing and reporting personal data breaches;

- in conducting data protection impact assessments and prior consultations with the supervisory authority.

If 2BITS receives a request concerning personal data processed solely on behalf of the Customer, it will forward the request to the Customer without undue delay and will not respond independently unless instructed to do so by the Customer or required to respond by law.

Assistance beyond the standard scope of the Services may be subject to an additional fee where it results from the Customer's actions or requires material involvement on the part of 2BITS.

8. Personal Data Breaches

Upon becoming aware of a personal data breach concerning personal data processed on behalf of the Customer, 2BITS will notify the Customer without undue delay.

To the extent that information is available, the notification will describe the nature of the breach, its possible consequences, the remedial measures taken or proposed and the contact point details. Information may be provided in phases.

The Customer is responsible for assessing whether the breach must be reported to the supervisory authority and communicated to data subjects, unless an obligation of 2BITS arises directly under applicable law.

9. Audits

2BITS makes available to the Customer the information necessary to demonstrate compliance with the DPA, in particular through documentation, responses to reasonable questionnaires, reports or available security materials.

If that information is insufficient, the Customer may conduct an audit itself or through an independent auditor bound by confidentiality, no more than once per year, unless a material breach has occurred or more frequent inspection is required by a supervisory authority.

The timing, scope and manner of the audit must be agreed in advance. The audit must not disrupt the operations of 2BITS, reduce the security of the Platform or infringe the rights of other customers. The Customer bears the costs of the audit unless the audit identifies a material breach of obligations by 2BITS.

10. Return and Deletion of Personal Data

During the term of the Agreement, the Customer may use the available data export features.

After the provision of the Services ends, 2BITS, at the Customer's choice and to the extent provided for in the Agreement, returns or deletes the personal data and any copies thereof, unless applicable law requires continued storage.

Personal data may remain in backups for a limited period. During that period, it remains protected, is not used for other purposes and is deleted in accordance with the normal backup retention cycle.

11. Final Provisions

In the event of any conflict between the DPA and other documents comprising the Agreement, the DPA takes precedence with respect to the processing of personal data.

The Parties' liability in connection with the DPA is subject to the rules and limitations set out in the Agreement, without prejudice to mandatory provisions of applicable law.

The DPA remains in force for as long as 2BITS processes personal data on behalf of the Customer.

Annex 1 – Description of Processing

Subject matter of processing: personal data entered into the Platform or provided to 2BITS by the Customer in connection with the provision of the Services.

Purpose of processing: making available, maintaining, securing and supporting the Platform, including the management of Users, training, enrolments, progress, results, certificates, communications, reports, integrations and technical support.

Nature of processing: collection, recording, organisation, storage, consultation, use, transmission, restriction, deletion and other operations necessary to provide the Services.

Duration: for the term of the Agreement and for the period necessary to return or delete the personal data.

Categories of data subjects: Platform Users, in particular employees, contractors, candidates, customers, partners, training participants, instructors and Customer administrators.

Categories of personal data:

- identification, contact and professional data;
- account data, roles and permissions;
- data concerning enrolments, participation, progress, results, attendance and certificates;
- content, statements, assignments, responses and attachments submitted by Users;
- technical data, identifiers, logs and activity information;
- data included in support requests;
- other data determined by the Customer and entered into the Platform.

Annex 2 – Technical and Organisational Measures

2BITS implements measures appropriate to the risk, the nature of the Services and the state of the art, including in particular:

- encryption of data in transit;
- access controls based on roles and the principle of least privilege;
- authentication and session management mechanisms;
- separation of Customer environments and data in accordance with the Platform architecture;
- event logging and operational and security monitoring;
- backups and data restoration procedures;
- update, configuration and vulnerability management;
- incident response and business continuity procedures;
- granting, reviewing and revoking personnel permissions;
- confidentiality obligations and training for persons with access to personal data;
- periodic reviews of the effectiveness of the safeguards implemented.

Document Information

- **Version:** 5.0
- **Effective date:** 1 August 2026
- **Last updated:** 2 July 2026
- **Document owner:** 2BITS