1. Issue:	14. 05. 2026	**Valid from:**	14. 05. 2026
Approved	**Yuri Schneiberg**	**Version no.:**	05

General Personal Data Protection Policy

CONTENT

1 SUMMARY

1.1 Purpose

For a company engaged in worldwide activity such as LearnQuest, modern information and communication technology is an important element in the implementation of business processes. The incorrect or improper use of this technology can lead to the infringement of personal rights. In the design of the information landscape, LearnQuest is pursuing the object of ensuring the personal rights of employees, customers, business partners, suppliers, stakeholders and other data subjects.

The objective of the procedure is to establish data protection and data security standards within LearnQuest that are uniform worldwide, fit for purpose and global, to satisfy the requirements arising from the European General Data Protection Regulation and other national adaptation laws.

1.2 Scope

The procedure applies to all processing and communication processes of LearnQuest. The organizational scope of the procedure applies to LearnQuest worldwide.

2 DEFINITIONS

Concept	*Definition*
Company, Organization	LearnQuest Incorporated
Personal data (PD)	means any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a 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 (SPD)	are racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.
Processing	means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Communication or transfer of personal data	is the disclosure of personal data to a third party in such a way that the data or forwarded to the third party or the third party views or retrieves the data held for viewing or retrieval.
Automated individual decisions	are decisions made by mechanical means only without assessment by a natural person

Restriction	'of processing' means the marking of stored personal data with the aim of limiting their processing in the future.
Data Subject	means any identified or identifiable natural person whose data are processed.
Controller	means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
Processor	means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Recipient	means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.
Data Protection Officer (DPO)	is an enterprise security leadership role required by the General Data Protection Regulation (GDPR). Data protection officers are responsible for overseeing a company's data protection strategy and its implementation to ensure compliance with GDPR requirements.
Guarantees	in the sense of this procedure are the rights and freedoms of the data subjects or the protective mechanisms carried out in order to secure personal rights.
Third party	means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data.
Third countries	are all states that are not members of the European Union (EU) or European Economic Area (EEA).
Binding corporate rules	means personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity.
Cross-border processing'	is a, processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or b, processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely

	to substantially affect data subjects in more than one Member State.
International organization	means an organization and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries.
Anonymization	is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable'. The GDPR does not apply to anonymized information.

3 VALIDITY OF PERSONAL LAW

The permissibility of the processing of personal data is judged on the basis of the General Data Protection Regulation and the specifically applicable national law. Where national legal regulations prescribe a higher level of data protection for personal data, these take precedence over the procedure. Each company of LearnQuest (their Affiliates) must check whether such regulations exist and ensure their compliance.

If a company of LearnQuest determines that parts of the procedure for the General Data Protection Regulation or national data protection law contradict and, within the framework of its obligations, prevent compliance with the procedure or the national law impairs the guarantees offered by the procedure in some other way, the Data Protection Officer must be brought into involvement.

4 THE HANDLING OF PERSONAL INFORMATION PRINCIPLES

4.1 Lawfulness

The processing of personal data is carried out lawfully, in good faith and in a manner that is accessible to the data subject, if at least one of the following preconditions is fulfilled:

a) The data subject has given consent for the processing for one or more specific purposes;

b) The processing is necessary for the fulfilment, implementation or termination of a contract or for the performance of precontractual measures;

c) The processing is necessary for a decision on the justification, after justification on the implementation or termination of the employment relationship or for the exercise or fulfilment of the rights and duties resulting from a collective agreement relating to the representation of the interests of personnel.

d) The processing is permissible for the detection of serious infringement of duties or offences by personnel, if actual indications to be documented justify the suspicion that the data subject has committed a serious infringement of duty or offence in the employment relationship, the processing is necessary for detection and the lawful interests of the personnel do not outweigh the exclusion of processing and, in particular, their nature and extent are not disproportionate in respect of the matter;

e) The processing is necessary for the fulfilment of a legal obligation;

f) The processing is necessary for the protection of the vital interests of the data subject or another natural person;

g) The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority;

h) The processing is necessary for the safeguarding of the lawful interests of the controller (e.g., a company of LearnQuest) or a third party, where the interests or basic rights and basic freedoms of the data subject do not outweigh these.

4.2 Sensitive Personal Data

The processing of sensitive personal data is fundamentally prohibited. LearnQuest doesn't process any kind of customer's SPD.

The following exceptions can be applied:

a) The data subject has given explicit consent to the processing of personal data for one or more specific purposes.

b) The processing is necessary in order that the controller or a data subject can exercise the rights arising from labor law and the law of social security and social protection and can fulfil their duties in this respect, where this is permissible in accordance with a legal provision or collective agreement.

c) The processing is necessary for the protection of the vital interests of the data subject and the data subject is incapable for physical or legal reasons of giving their consent.

d) The processing relates to data that the data subject has manifestly made public.

e) The processing is necessary for the enforcement, exercise, or defense of legal claims or in action of the courts within the scope of their judicial activity.

f) The processing is necessary for reasons of major public interest.

g) The processing is necessary for the purposes of health care or occupational medicine. These include

1. assessment of the ability to work of personnel,
2. medicinal diagnostics,
3. provision or treatment in the field of health or social care or,
4. the administration of systems and services in the field of health or social care.

These data may only be processed by skilled personal or acting under their responsibility if these skilled personnel are subject to professional confidentiality or the processing is carried out by another person who is subject to a duty of confidentiality.

4.3 Definition of Purpose

Personal data may only be processed for purposes that are defined, unambiguous and lawful.
A change of purpose is fundamentally only permissible if the processing is reconcilable (compatible) with those purposes for which the data was originally collected, or the data subject has consented to the change of purpose.

4.4 Duty of Transparency and Information

4.4.1 Duties of Transparency and Information in Direct Collection

In accordance with the principle of direct collection, personal data must fundamentally be collected from the data subject themselves. The controller informs the data subject of these data of the following:

a) the name and contact information of the Controller;

b) the contact information of the Data Protection Officer;

c) the purposes and the legal basis of the processing;

d) if the processing is based on section 4.1 of this procedure, the justified interests that are being pursued by the controller or a third party;

e) the recipients of categories of recipients;

f) the intention of the controller to communicate the data to a third country, as well as the presence or absence of an appropriate level of data protection or appropriate guarantees and the possibility of viewing evidence thereof;

g) the duration of storage of the personal data or, if this is not possible, the criteria for defining the storage duration;

h) the existence of the rights of data subjects in accordance with section 8 of this procedure,

i) if the processing is based on consent, the right to withdraw this consent at any time, whereby the legitimacy of the processing carried out is not affected on the basis of the consent until its withdrawal;

j) the existence of any automated decision making process including profiling in accordance with section 4.7 of this procedure, meaningful information on the logic involved and the scope and sought effects of such processing and

k) whether the provision of the personal data is prescribed by law or by contract or is necessary for conclusion of a contract, the data subject is obliged to provide the personal data and the possible consequences that would be brought about by failure to provide the data.

If the controller intends to process the personal data further for a different purpose than the original purpose, he shall provide the data subject in advance of this further processing with the information in accordance with section 4.4.1 g – k of this procedure.

The controller shall give this information within an appropriate deadline period after acquisition of the personal data, but within a maximum of one month. If the personal data is to be used for communication with the data subject, no later than the time of the first message to the data subject or, if the intention is to disclose the information to another recipient, no later than the time of the first disclosure.

4.4.2 Form of Implementation of the Duties of Transparency and Information

The controller shall take suitable measures in order to the communicate all information to the data subject in a precise, transparent, comprehensible and easily accessible form and in clear and simple language. The information shall be communicated in written or electronic form.

4.4.3 Exceptions from the Duty of Transparency and Information

There is no duty to inform the data subject if the data subject already possesses the information or the generally acknowledged business purposes of LearnQuest would be substantially endangered and this is not outweighed by the interest of the data subject in the provision of information.

There is no duty to inform the data subject in the case of collection from third parties:

a) if the provision of the information proves to be impossible or would require disproportionate outlay; this applies in particular where the information prevents or seriously impairs the realization of the objectives of this processing or

b) the personal data is subject to professional confidentiality, including a statutory duty of confidentiality.

4.5 Accuracy

Personal data must be accurate and current. Appropriate measures must be taken in order that personal data that is incorrect in relation to the purposes of its processing is deleted or corrected without delay.

4.6 Minimization of data and restriction of storage

Personal data must be appropriate to the objective, necessary and its quantity restricted to the minimum necessary for the purposes of processing. The principle shall apply as little as possible, as much as necessary.

The personal data must be stored in such a form that allows identification of the data subjects for only so long as is necessary for the purposes for which the data is processed.

4.7 Automatized individual decision-making including profiling.

If personal data is processed with the objective of achieving automatic decision making, including profiling, the justified interests of the data subject shall be ensured by means of suitable measures.

If processing has a legal effect on a data subject, or if this person is substantially compromised in a similar manner by processing, this decision shall not be based exclusively on an automated individual decision or profiling.

An exception only applies if:

a) the decision to conclude or fulfil a contract between the data subject and the controller is necessary.

b) the decision is permissible based on legal regulations or

c) the decision is made with the explicit consent of the data subject.

In the case of decisions in accordance with section 4.7 a and c of this procedure, the controller takes appropriate measures to secure the rights and freedoms as well as the justified interests of the data subject. This includes the right of the data subject to state their position and contest the decision.

5 DATA SECURITY

The Data Protection Impact Assessment - DPIA (Privacy Impact Analysis) must be carried out if there is a risk in the processing of personal data to the rights and freedoms of the data subject. In this case, suitable technical and organizational measures must be defined for the protection of the data subject.

These measures are determined based on risk and covering the data categories to the processed taking account of the type, scope, circumstances, purposes, and functionalities of the processing, as well as the state of the art and the implementation costs.

The measures are derived from the guidelines and procedures for IT security and information security of LearnQuest and include matters such as the following:

a) the pseudonymization or encryption of personal data.

b) the ability to ensure the confidentiality, integrity, availability and resilience of the systems and services in

connection with the processing in the long term.

c) the ability to rapidly restore the availability of the personal data and access thereto in the case of a physical or technical incident and

d) a process for the regular checking, assessment, and evaluation of the effectiveness of the technical and organizational measures for ensuring the security of processing.

The data protection impact assessment must be performed and documented before the commissioning of processing and in the development of products and services (Privacy by Design).

In the case of products and services, the pre-setting's must be selected in a data protection-friendly way in accordance with the principles of data avoidance and minimization. These measures must ensure in particular that personal data are not made accessible to an indeterminate number of natural persons by the pre-setting's without the intervention of the data subject and only those personal data are processed that are necessary for the specific purpose (Privacy by Default).
For the data protection impact assessment of several similar cases of processing of personal data with similar risks, a single such analysis may be carried out.

6 RECORDS OF PROCESSING ACTIVITIES

The Affiliates of LearnQuest in the EU maintain a directory of processing activities for all cases of processing of personal data. This is used to record, in particular, the following information on each case of processing:

1. the name and contact information of the controller and any Data Protection Officer,
2. the purpose of the processing,
3. the categories of the data subjects and categories of the personal data,
4. the categories of the recipients,
5. a statement as to whether data processing is subcontracted,
6. statements on communications to third countries and forwarding of data,
7. statements on authorization concepts and erasure requirements,
8. statements on data security and IT security,
9. data protection impact assessment.

This complies with the essential duties of documentation and accountability in data protection law.

6.1 Data Retention and Storage Management

6.1.1 General Principle of Retention and Storage

Personal data shall be stored 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.

Retention periods are determined taking into account:

1. the purpose of processing,
2. applicable legal and regulatory requirements,
3. contractual obligations, and
4. the legitimate interests of LearnQuest, provided such interests do not override the rights and freedoms of the data subject.

Where personal data is no longer required, LearnQuest will take reasonable steps to delete or anonymize such data in accordance with applicable procedures.

6.1.2 Retention Framework

LearnQuest applies standard retention timeframes to commonly processed categories of personal data. These timeframes are intended to guide consistent handling of personal data across systems and functions.

Data Category	**Retention Period**	**Legal Justification**
Payment & transaction records	7 years	Tax/legal obligations
Certification/educational records	10 years	Accreditation & compliance
Account data (inactive)	5 years of inactivity	Legitimate interest / business need
Marketing data	Deleted 24 months after the later of the last marketing email engagement (e.g., link click) or most recent consent renewal	Consent
Support inquiries	24 months	Legitimate interests
Analytics & advertising event data	GA4 default (14 months); aggregated de-identified metrics retained longer where permissible	Platform settings & de-identified use

These retention periods may vary depending on the specific processing activity, system constraints, or applicable legal requirements.

Retention may be extended where necessary to:

1. comply with legal or regulatory obligations,
2. establish, exercise, or defend legal claims, or
3. support legitimate interests consistent with applicable law. Con

6.1.3 Storage of Personal Data

Personal data may be stored and processed within:

1. LearnQuest internal systems,
2. cloud-based platforms and service providers, and
3. systems operated by authorized processors.

Such systems may be located in jurisdictions where LearnQuest or its service providers operate, subject to appropriate safeguards as described in this procedure.

LearnQuest implements technical and organizational measures designed to protect personal data and restrict access to authorized personnel.

6.1.4 Deletion and Anonymization

LearnQuest seeks to ensure that personal data is not retained longer than necessary.
Where appropriate, personal data is:

1. deleted from active systems, or
2. anonymized so that it can no longer be associated with an identifiable individual.

Deletion and anonymization are carried out in accordance with operational practices and system capabilities, recognising that timing and implementation may vary across systems.

6.1.5 Backup and Archival Data

Personal data may be included in system backups and archival systems for business continuity and disaster recovery purposes.
Such data:

1. is not routinely accessed or used for active processing, and
2. is retained in accordance with applicable IT and security practices.

Where personal data is deleted from active systems, residual copies may remain in secure backups for a limited period before being overwritten in the normal course of operations.

6.1.6 Responsibility and Oversight

Responsibility for data retention and storage is shared across LearnQuest functions, including:

1. relevant business and process owners, who determine data use and retention needs,
2. IT and system administrators, who support implementation of storage and deletion practices, and
3. compliance or privacy personnel, who provide oversight and guidance.

Retention practices are documented, reviewed periodically, and updated as necessary to reflect changes in legal requirements or business operations.

6.1.7 Exceptions and Legal Requirements

In certain circumstances, personal data may need to be retained beyond standard timeframes, including where required for:

a) legal or regulatory obligations,
b) litigation or investigations, or
c) enforcement of legal rights.

In such cases, deletion may be suspended until the relevant requirement has been satisfied.

7 DATA TRANSFER

7.1 Data transfer in the EU/EEA.

The transfer of personal data within the LearnQuest or to an external company with a head office in the EU/EEA is permissible if the data processing is permissible in accordance with section 4.1 of this procedure.

7.2 Data transfer to Third Countries

The transfer of personal data within the LearnQuest or to an external company with a head office in a third country is permissible if the data processing is permissible in accordance with section 4.1 of this procedure and one of the following conditions is fulfilled:

a) the transfer is necessary for the fulfilment of a contract between the data subject and the controller or for the implementation of precontractual measures at the instigation of the data subject.

b) the transfer is necessary for the conclusion or fulfilment of a contract concluded in the interest of the data subject by the controller with another natural or legal person.

c) the transfer is necessary or prescribed in law for the securing of an important public interest or for the enforcement, exercise, or defense of legal claims before a court.

d) the transfer is necessary for the protection of the vital interests of the data subject or other persons, where the data subject is incapable for physical or legal reasons of giving their consent.

e) the transfer is carried out to a third country for which the EU Commission has defined an appropriate level of data protection or

f) the controller or processor has provided suitable guarantees, particularly within the scope of legal agreements by the current and valid EU Standard Contractual Clauses or Binding Corporate Rules that ensure that a corresponding standard of data protection is guaranteed.

the data subject has given their consent after they have been briefed on the existing possible risks of such data communications to a third country without the presence of an adequacy decision by the EU Commission and without suitable guarantees.

7.3 Onward Transfer of Personal Data

The onward transfer of personal data from the EU/EEA within a third country or from a third country to another third country is only permissible if the requirements in section 4.1 and section 7.1 of this procedure are observed. The company of the LearnQuest in the EU/EEA that has transferred the data must be informed of such a transfer. In this case, the company of the LearnQuest has a right to object to the data transfer.

7.4 Processing

If a company (Affiliate) of the LearnQuest uses a processor for performing activities, the following points must be observed:

1. The principal shall work only with agents who offer sufficient guarantees that suitable technical and organizational measures are implemented in such a way that the processing is carried out in accordance with the requirements of this procedure and ensure the protection of the rights of the data subjects.

2. The agent shall not consider any other processors (subcontractors) without the prior written authorization of the principal. If the agent for carrying out certain processing activities is permitted to consider the services of a further processor on behalf of the principal, the same data protection duties are applied to the further processor as between the agent and the principal.

3. The processing by an agent is carried out on the basis of a contract that binds the agent vis-a-vis the principal and that defines the object and duration of the processing, the type and purpose of the processing, the type of personal data, the categories of the data subjects and the duties and rights of the principal. This contract shall provide in particular that the agent:

    a) processes the personal data only at the documented instruction of the principal.

    b) ensures that the persons authorized for the processing of the personal data are subject to a duty of confidentiality.

c) supports the principal in his duty to apply suitable technical and organizational measures in the answering of applications to preserve the rights of data subjects.

d) supports the principal in compliance with his duties, especially in ensuring the security of processing, the notification of infringements to the regulatory body, notification of the person affected by an infringement, in the implementation of the data protection impact assessment and any consultation resulting therefrom with the data protection authority in processing of high risk.

e) deletes or surrenders all personal data after completion of the service performance according to the decision of the principal, unless there are legal duties of storage and

f) provides the principal with all necessary information for demonstration of the duties regulated in the contract and facilitates and contributes to any inspections that are carried out by the principal or another inspector instructed by the principal.

If this agent has a head office in a third country and has not provided suitable guarantees or an appropriate level of data protection has not been defined by the EU commission, the current and valid EU Standard Contractual Clauses (Controller to Processor) must additionally be concluded.
In this case, it is immaterial whether the processor is a company of LearnQuest or an external company.

8 RIGHTS OF DATA SUBJECTS

Data subjects can, in relation to the processing of their personal data, enforce a large number of rights vis-a-vis the controller. The enforcement of these rights must be processed without delay by the controller.

8.1 Right of Access

The data subject may request confirmation from any company of LearnQuest as to whether their personal data are being processed. They have a right to access the following information:

a) the purposes of the processing;

b) the categories of personal data;

c) the recipients or categories of recipients, in particular in the case of recipients in third countries;

d) the planned duration for which the personal data will be stored or, if this is not possible, the criteria for defining this duration;

e) the existence of a right to rectification, erasure or restriction of the processing and a right to object to this processing as well as the existence of a right to appeal to a data protection authority;

f) the origin of the data;

g) the existence of any automated decision making process including profiling in accordance with section 4.7 of this procedure and meaningful information on the logic involved as well as the scope and sought effects of such processing for the data subject and

h) the suitable guarantees implemented by the controller in the communication of personal data to a third country.

The information must be communicated in a precise, transparent, comprehensible and easily accessible form in clear and simple language. The controller shall provide the data subject with the information within a month of receipt of the request. Requests for information should where possible be answered by electronic means. The controller shall

provide free of charge a copy of the personal data that is the object of the processing. For further copies, the controller may request an appropriate payment on the basis of the administration costs incurred.

The right to information ceases to apply if

a) this is permissible in accordance with the applicable national law for LearnQuest company processing data or communicating data or

b) the data are only therefore stored since they must not be deleted as a result of legal or contractual storage specifications or

c) are exclusively for the purposes of data security or data protection control and the provision of information would require disproportionately large outlay and the processing for other purposes is excluded by means of suitable technical and organizational measures or

d) if this would be associated with a substantial risk to business purposes, such as the disclosure of trade secrets and the interest in securing trade secrets outweighs the interest in the information interest of the data subject.

The reasons for a refusal of information must be documented. A reason for the refusal to provide information must be given to the data subject, where the purpose pursued with the refusal to provide information would not be put at risk through the provision of the actual and legal reasons on which the decision is supported. The data stored for the purpose of providing information to the data subject and for their preparation may only be processed for this purpose and for the purposes of data protection control.

8.2 Right to Object

The data subject has the right to lodge an objection at any time to the processing of the personal data affecting them that is carried out on the basis of section 4.1 a or h or section 4.7 of this procedure or are processed for the purposes of direct publicity. If the data subject uses their right to object, the controller must no longer process these personal data, unless the controller can demonstrate lawful grounds for the processing that outweigh the interests, rights and freedoms of the data subject or the processing serves in the enforcement, exercise or defense of legal claims.

The right to object covers all data processing extending into the future. The data subject must be explicitly alerted to the right to object no later than the time of the first communication with them. This information must be given in a comprehensible form separately from other information.

8.3 Right to Rectification

Any data subject has the right to request from the controller the rectification of the personal data affecting them if these are not correct. Taking account of the purposes of the processing, the data subject has the right to request the completion of personal data.

8.4 Right to Restriction

The data subject has a right to request from the controller the restriction of processing if one of the following preconditions applies:

a) the accuracy of the personal data is disputed by the data subject, and namely for the duration that allows the controller to check the accuracy of the personal data.

b) the processing is unlawful, and the data subject declines the erasure of the personal data and instead requests the restriction of the use of the personal data;

c) the controller no longer requires the data, but the data subject requires the data for the enforcement, exercise or defense of legal claims or

d) the data subject has lodged an objection to the processing and namely and namely for the duration until it is determined whether the lawful reasons of the controller outweigh those of the data subject.

If the processing has been restricted, these personal data many only be processed – as distinct from their storage – with the consent of the data subject or for the enforcement, exercise, or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

8.5 Right to Erasure

The data subject has the right to request from the controller the erasure of the personal data affecting them and the controller is under a duty to delete personal data if:

1. the personal data are no longer necessary for the purposes for which they were collected or processed in some other way;

2. the data subject rescinds their consent upon which the processing is supported in accordance with section 4.1 a or section 4.2 a of this procedure and there is no other legal basis for processing;

3. the data subject lodges an objection in accordance with section 8.2 of this procedure to the processing and there are no overriding lawful grounds for the processing;

4. the personal data has been processed unlawfully or

5. the erasure of the personal data is necessary in order to fulfil a legal obligation to which the controller is subject.

If there are legal storage regulations, the data must be quarantined instead of being deleted.

8.6 Right to Data portability

The data subject has the right to receive the personal data that they have provided to a controller affecting them in a structured, conventional and machine readable format and has the right to communicate these data to another controller without hindrance by the controller to whom the personal data was provided, where the processing

1. is based on consent or a contract and

2. with the aid of an automated method.

Furthermore, the data subject can request where technically feasible that their personal data be communicated by a LearnQuest company to another controller.

8.7 Right to lodge a Complaint

Any data subject can lodge a complaint with the justification that a company of LearnQuest has breached the procedure. Appeals should be directed to the Data Protection Officer. Receipt of the complaint must be promptly

confirmed to the data subject and the complaint must be answered within an appropriate deadline period, but no later than one month from receipt of the complaint.

9 NOTIFICATION OF DATA PROTECTION INCIDENTS AND DATA PROTECTION BREACHES

Data protection incidents and data protection breaches must be notified without delay to the Data Protection Officer. He decides in consultation with management whether this incident or breach should be notified to the responsible data protection authority.

The Data Protection Officer of LearnQuest should be contacted as follows: Privacy.Compliance@LearnQuest.com

10 REFERENCES

This section lists the sources consulted to create this policy.

- *GDPR*
- *ISO 27701:2018*