DATA PROTECTION

Introduction

Scaling Room is committed to providing a superior learning experience for everyone we work with. We know that our users' are committed to their success and we are equally committed to ensuring that each interaction that someone has with our content is optimized for maximum educational potential. To enable us to do this, Scaling Room needs to gather and use certain information about individuals.

Individuals who we gather information about includes customers, affiliates, business contacts, employees, and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data is collected, handled, and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures Scaling Room:

Complies with data protection law and follows industry best practices

Protects the rights of staff, customers, affiliates, and partners

Is open about how it stores and processes individuals' data

Protects itself from the risks of a data breach

Eu general data protection regulation (gdpr) protection law

The GDPR (General Data Protection Regulation) protection law describes how organizations who conduct business with individuals or entities located in EU (European Union) nations — including Scaling Room — must collect, handle, and store personal information.

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

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

The EU GDPR is underpinned by eight core principles. These state that personal data must:

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

1. policy statement

Every day our business will receive, use, and store personal information about our customers, affiliates, partners, and colleagues. It is important that this information is handled lawfully and appropriately, in line with the requirements of the Data Protection Act 2018 and the General Data Protection Regulation (collectively referred to as the 'Data Protection Requirements').

We take our data protection duties seriously, because we respect the trust that is being placed in us to use personal information appropriately and responsibly.

2. about this policy

This policy and any other documents referred to in it, sets out the basis on which we will process any personal data that we collect or process. This policy does not form part of any employee's contract of employment and may be amended at any time.

The company as a whole is responsible for ensuring compliance with the Data Protection Requirements and with this policy. Any questions about the operation of this policy or any concerns that the policy has not been followed should be referred in the first instance to the Data Protection Officer.

3. what is personal data?

Personal data is defined as data, (whether stored electronically or paper based) relating to a living individual who can be identified directly or indirectly from that data, (or from that data and other information in our possession).

Processing is any activity that involves use of personal data. It includes obtaining, recording, or holding the data, organizing, amending, retrieving, using, disclosing, erasing, or destroying it. Processing also includes transferring personal data to third parties under privacy control conditions.

Sensitive personal data includes contact info, address, session activity on the platform, IP location etc. Sensitive personal data can only be processed under strict conditions, and used for express purpose that it was collected for.

4. data protection principles

Anyone processing personal data, must ensure that data is:

- Processed fairly, lawfully and in a transparent manner.
- Collected for specified, explicit, and legitimate purposes and any further processing is completed for a compatible purpose.
- Adequate, relevant and limited to what is necessary for the intended purposes.
- Accurate and where necessary, kept up to date.
- Kept in a form which permits identification for no longer than necessary for the intended purposes.
- Processed in line with the individual's rights and in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.
- Not transferred to people or organizations situated in countries without adequate protection and without firstly having advised the individual.

5. fair and lawful processing

The Data Protection Requirements are not intended to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the individual.

In accordance with the General Data Protection Regulation (GDPR), we will only process personal data where it is required for a lawful purpose. The lawful purposes include (amongst others): whether the individual has given their consent, the processing is necessary for performing a contract with the individual, for compliance with a legal obligation, or for the legitimate interest of the business. When sensitive personal data is being processed, additional conditions must be met.

Collection of Information

We receive and store information about you such as:

Information you provide us: We collect information you provide to us which includes: your name, email address, address or postal code, payment method, and telephone number. We collect this information in a number of ways, including manual entry while you are using our service, interact with our customer service, participate in surveys or marketing promotions, provide reviews or ratings, taste preferences, set preferences in Your Profile/Account, or otherwise provide information to us through our service or elsewhere.

Information we collect automatically: We collect information regarding you and your use of our service, your interactions with us and our advertising, as well as information regarding your computer or other device used to access our service.

This information includes:

- Your activity on our platform such as course progress and search queries
- Details regarding your interactions with customer service such as the date, time and reason for contacting us
- Transcripts of any chat conversations that you initiate on our platforms
- In the event that you initiate phone support, your phone number
- Device IDs or unique identifiers, device and software characteristics (such as type and configuration)
- Connection information, statistics on page views, referral URLs, IP address, and standard web log information
- Information collected via the use of cookies, web beacons and other technologies, including ad data (such as information on impressions delivered to a cookie, the site URL where the impression was delivered, as well as the date and time).

See our Privacy Policy for more details.

Use of Information

We use the information we collect to provide, analyze, administer, enhance, and personalize our services and marketing efforts, to process your registration, your orders, your payments, and your communication on these and other topics.

Our primary aim is always to enhance the user experience. We do so in several ways using the data that we collect, but a few examples are: determining your general platform usage, required action item completions, login details, etc. which then helps us know what difficulties the you're facing within the platform, with which can then use to take action to minimize the effort on your end. We collect other information, such as most visited links on our website, which then help us conclude what content was most watched, enabling us to create additional content geared toward our users' needs and personal preferences.

6. processing for limited purposes

In the course of our business, we may collect and process personal data, which may include data that we receive directly from a data subject and data we receive from other sources including location data, business partners, and subcontractors who work technical, payment and delivery services, credit reference agencies, and other capacities.

We will only process personal data for the specific purposes or for any other purposes specifically permitted by the Data Protection Requirements. We will notify those purposes to the data subject when we first collect the data or as soon as possible thereafter.

7. notifying individuals

If we collect personal data directly from an individual, we will inform them about:

- The purpose or purposes for which we intend to process that personal data, as well as the legal basis for the processing.
- Where we rely upon the legitimate interests of the business to process personal data, the legitimate interests pursued.
- The types of third parties, if any, with which we will share or disclose that personal data.
- The fact that the business intends to transfer personal data to a non-EEA country or international organization and the appropriate and suitable safeguards in place.
- How individuals can limit our use and disclosure of their personal data.
- Information about the period that their information will be stored or the criteria used to determine that period.
- Their right to request from us as the controller access to and rectification or erasure of personal data or restriction of processing.
- Their right to object to processing and their right to data portability.
- Their right to withdraw their consent at any time (if consent was given) without affecting the lawfulness of the processing before the consent was withdrawn.
- The right to lodge a complaint with the Information Commissioner's Office.
- Other sources where personal data regarding the individual originated from and whether it came from publicly accessible sources.
- Whether the provision of the personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the individual is obliged to provide the personal data and any consequences of failure to provide the data.
- The existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the individual.

If we receive personal data about an individual from other sources, we will provide them with this information as soon as possible (in addition to telling them about the categories of personal data concerned) but at the latest within One (1) month.

We will also inform data subjects whose personal data we process, that we are the data controller with regard to that data and our contact detail regarding data protection act is support@scalingroom.com, and who the Data Protection Compliance Manager/Data Protection Office is.

8. adequate, relevant and non-excessive processing

We will only collect personal data to the extent that it is required for the specific purpose notified to the data subject.

9. accurate data

We will ensure that personal data we hold is accurate and kept up to date. We will check the accuracy of any personal data at the point of collection and at regular intervals afterwards. We will take all reasonable steps to destroy or amend inaccurate or out-of-date data.

10. timely processing

We will not keep personal data longer than necessary for the purpose or purposes for which it was collected. We will take all reasonable steps to destroy or erase from our systems, all data which is no longer required.

11. processing in line with data subject’s rights

We will process all personal data in line with data subjects' rights, in particular their right to:

- Confirmation as to whether or not personal data concerning the individual is being processed.
- Request access to any data held about them by a data controller.
- Request rectification, erasure or restriction on processing of their personal data.
- Lodge a complaint with a supervisory authority.
- Data portability.
- Object to processing including for direct marketing.
- Not be subject to automated decision making including profiling in certain circumstances.

12. data security

We will take appropriate security measures against unlawful or unauthorized processing of personal data and against the accidental or unlawful destruction, damage, loss, alteration, or unauthorized disclosure of or access to personal data transmitted, stored, or otherwise processed.

We will put in place procedures and technologies to maintain the security of all personal data from the point of the determination of the means for processing and point of data collection to the point of destruction. Personal data will only be transferred to a data processor if he or she agrees to comply with those procedures and policies, or if he or she puts in place adequate measures himself/herself.

We will maintain data security by protecting the confidentiality, integrity, and availability of the personal data, defined as follows:

- Confidentiality: Only people who are authorized to use the data can access it.
- Integrity: Personal data should be accurate and suitable for the purpose for which it is processed.
- Availability: Authorized users should be able to access the data if they need it for authorized purposes. Personal data should therefore be stored on the Scaling Room central computer system & databases instead of individual PCs.

Our Security Procedures:

- Entry controls: Any stranger seen in entry-controlled areas will be reported.
- Securing lockable desks and cupboards all the time. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- Data minimization will be practiced.
- Pseudonymisation and encryption of data will be the primary state of storing the data.

- Methods of disposal: Paper documents would be shredded. Digital storage devices would be physically destroyed when they are no longer required. Electronic data would be deleted once it's intended purpose is fulfilled.
- Equipment: Staff has to ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

Transferring Personal Data Outside of the EEA: We may transfer any personal data we hold to a country outside the European Economic Area ('EEA') or to an international organization, provided that one of the following conditions applies:

- The country to which the personal data is transferred ensures an adequate level of protection for the data subjects' rights and freedoms.
- The data subject has given his consent.
- The transfer is necessary for one of the reasons set out in the Act, including the performance of a contract between us and the data subject, or to protect the vital interests of the data subject.
- The transfer is legally required on important public interest grounds or for the establishment, exercise or defense of legal claims.
- The transfer is authorized by the relevant data protection authority where we have adduced adequate safeguards with respect to the protection of the data subjects' privacy, their fundamental rights and freedoms, and the exercise of their rights.

Subject to the requirements above, personal data we hold may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Those staff may be engaged in, among other things, the fulfilment of contracts with the data subject, the processing of payment details and the provision of support services.

14. disclosure and sharing of personal data

We may share personal data we hold with any member of our group, which means our subsidiaries, our ultimate holding company and its subsidiaries, as defined in: https://www.legislation.gov.uk/ukpga/2006/46/section/1159

15. subject access requests

To these ends, the company has a privacy statement setting out how data relating to individuals is used by the company.

Individuals must make a formal request for information we hold about them. Employees who receive a request should forward it to the data department immediately.

When receiving telephone enquiries, we will only disclose personal data we hold on our systems if the following conditions are met:

- We will check the caller's identity to make sure that information is only given to a person who is entitled to it.
- We will suggest that the caller put their request in writing if we are not sure about the caller's identity and where their identity cannot be checked.
- Where a request is made electronically, data will be provided electronically when possible.
- Our support team will refer a request to the data processing department or the Data Protection Compliance Manager for assistance in difficult situations.

16. changes to this policy

We may modify this Privacy Statement at any time, but we will provide prominent advance notice of any material changes to this Statement, such as posting a notice through the Services, on our websites, or sending you an email, to provide you the opportunity to review the changes and choose whether to continue using the Services.