# General Data Protection Regulation (GDPR)

*The General Data Protection Regulation, known as GDPR, was approved by the European Union in April 2016 and is scheduled to go into effect on* May 25, 2018. It is the most sweeping legislation in the last two decades focused on data security and privacy, and significantly updates, extends, and harmonizes data protection legislation across the EU/EEA.

**Who is subject to GDPR?**
Individuals, organizations and companies that control or process personal data are subject to GDPR. In broad terms, there are three different actors:

- Data subjects (students, families, school employees)
- Data controllers (the school)
- Data processors (school systems like Sycamore Education)

As a data processor, we do not decide the purpose or lawfulness of the data we process and store. We are trustees acting on our customers' behalf. As data controllers, schools remain ultimately responsible for documenting and deciding how data enters our systems. However, GDPR regulations do impose new and stricter regulations on processors.

**How is GDPR different from current data protection laws?**

Key areas of difference center on increased accountability for companies, greater access to personal data for individuals, and higher penalties for non-compliance.

GDPR explicitly lays out key rights of data subjects:

- right to be informed
- right of rectification
- right of erasure
- right of restrict processing
- right of data portability
- right to object
- right of access

These rights form the framework for interactions between the data subject, controller, and processor. While the controller (school) remains responsible for respecting these rights, the processor (Sycamore Education) may assist in accomplishing these tasks.

The penalties for non-compliance are not insubstantial. A school found in violation of GDPR may be assessed fines worth up to 4% of total annual revenue. The Supervisory Authorities (SA's) in each member state are responsible for enforcing GDPR and has a broad range of powers to do so.

**What kind of data is covered, and what information are schools allowed to collect?**

All personal data concerning an individual (data subject) is included under GDPR. Specifically, personal data that allows an individual to be identified — for example name, address, phone number, photo, etc. — is included under GDPR.

Even if personal data has been encrypted, pseudonymised, or anonymized, it may still fall under the scope of GDPR if the data can still be used to identify a specific individual.

Examples of personal data that our schools collect and store includes:

- Names
- Addresses
- E-mail Addresses
- Phone numbers
- ID Numbers (passport, national ID, SSN)

GDPR specifies six lawful bases for collecting personal data:

- Consent
- Written contract
- Legal Obligation
- Vital interests
- Public tasks
- Legitimate interests

For most schools, the legal basis for data collection relates to either legal obligations as learning institutions, or to legitimate interests.

Most of the bases require that the data processing is necessary, i.e. if you can reasonably achieve the same results and purpose without processing data, then you do not have a lawful basis.

**Is Sycamore Education GDPR-compliant?**

We will be as of May 25, 2018. We are well prepared for the upcoming GDPR changes with a strong set of organizational and technical security measures. Sycamore Education has been designed from the start with personal data protection in mind, and offer schools, students, and parents a secure platform.

GDPR does not specify precise security requirements for cloud-based services. As a data processor, we have shared responsibility with our schools (controllers) to provide organizational and technical security, and be able to demonstrate it. GDPR strengthens the liabilities and penalties for companies that unable to demonstrate those security protocols.

Since the beginning, Sycamore Education has successfully protected data for our users. We continue to invest in organizational security, network and infrastructure security, as well as application security to ensure we can offer world-class security beyond standard requirements.

- We are careful not to provide explicit detail about our security measures but our standard protocols include:
- Application security: End to end traffic encryption, strongly hashed passwords, safeguards against vulnerabilities such as cross site scripting, SQL injections, phishing and others.
- Network Security: firewalls and systems to detect suspicious behavior, stop malicious attempts to gain access, or compromise the resilience of the service (e.g. DDOS attacks).
- Organizational security: access policies, audit logs and confidentiality agreements.
- Physical security: preventing unauthorized access to infrastructure processing personal data.
- Procedural security: IT management processes to minimize the risk of human errors, or testing regimes to identify software weaknesses before releasing new features to our cloud services, or policies to ensure data is only processed in instruction from our customers.

As a part of our commitment to GDPR, you can expect Sycamore Education to:

- Ensure organizational and technical security for all services.
- Assist with documentation to demonstrate compliance and keep users informed.
- Provide new contract addenda that comply with GDPR requirements for Data Processing Agreements (DPA).
- Offer support when your users exercise their data subject rights.

**How does my school become GDPR-compliant?**

We cannot directly advise our schools on GDPR compliance, aside from recommending that you seek legal advice as soon as possible, and appoint a team to begin reviewing your current data processing practices. Most of our schools in Europe will be required to appoint a Data Protection Officer (DPO), who oversees your compliance requirements and reports directly to senior management.

In general, GDPR will require you to explicitly record and evaluate how personal data is processed and used. At a minimum, you will need to fully review user data end-to-end, justify why you hold it (using one of the legal bases), for how long you will retain it, and conduct a security review. The purpose of every data point you hold must be defined.

When adopting new technology platforms that involve personal data, you will need to perform a Data Protection Impact Assessment (DPIA). You are expected to monitor and ensure that the systems you use are GDPR compliant.

Lastly, because individual rights have been strengthened under GDPR, we strongly recommend making your users aware of their rights, and establishing clear procedures for responding when users exercise those rights.

**How does Sycamore Education obtain personal data about users, and how is it used?**

User data is submitted to our platforms in three ways:

1. directly by the users
2. by representatives authorized by the users (e.g. the school administration obtains data and then uploads it to our platform)
3. via an external document from a third-party system

Data typically enters our systems via “student information systems” independently maintained and controlled by our customer schools. We import data from third-party systems only under direct instruction from our customers.

We use personal data under our protection only when we receive direct instructions from the customer school. The data stored on our systems belongs directly to our customers, and only Sycamore Education support staff have access to personal data under strict confidentiality and security. We process personal data independently only if it is vital to the integrity or security of the service, or to analyze or evaluate the quality of the service provided.

**Can any of our users request data deletion under the “right to be forgotten”?**

Likely not. A data deletion request is valid only if the lawful basis of the processing is Consent (see above), or if the original purpose is no longer valid.

We strongly recommend that our schools implement clear processes for evaluating these kinds of requests. Our Data Protection Officer can also assist with advice in difficult cases. If a data subject is granted the right to be deleted, Sycamore Education will, either through our software or our support services, help execute these rights and confirm the deletion.

**When does Sycamore Education delete personal data?**

Sycamore Education deletes personal data when instructed by our customers, or if the contract between us and the customer is terminated. The procedures around deleting customer data upon termination of service should be provided in writing or in a Data Processor Agreement.

An instruction to delete a user in our services can either be manually performed in the platform by a customer representative or upon request to our support team.

When users are deleted in our systems, there are safeguards in place to prevent errors leading to an irreplaceable loss of data. In many cases customers will have to manually confirm the deletion of customer data, including personal data.

**Are we required to provide the personal data that we store on a user when requested?**

To a limited degree, yes. Your users have strong rights to transparency, information, and data access. Any data subject can request a copy of all personal data stored, provided that it does not adversely impact other users, or if the data is not already directly available.

Please note this is not an absolute right. There are other laws in place that require you to protect the data subject and others from accessing certain kinds of information. Again, we strongly recommend that you implement a clear process for evaluating this kind of request, and our Data Protection Officer can assist in difficult cases. If you grant a data subject the right of access, we will, either through our software or our support services, help execute these rights.

Our systems were built for transparency across all stakeholder groups, so the majority of data stored about a user is directly accessible via the individual user profile.

**Can a user contact Sycamore Education directly (e.g. student, parent, teacher) to exercise his rights under GDPR?**

No. Under GDPR, the data subject (user) rights is between him/her and the controller (our customers). Any data subject requests from end users to Sycamore Education will be handed over to the customer. Sycamore Education will cooperate in good faith with customers to ensure they can exercise the rights of the data subjects in a prompt manner.

**Does Sycamore Education send data to third parties?**

No, unless we receive instruction / confirmation from our customers or have a legal obligation to do so.

Schools often request that we integrate with a third-party tool or service, or they setup this integration directly themselves using our publicly available API. We take steps to prevent customers from sending data to 3rd parties without complying with data protection regulations. However, it is important that our customers themselves implement safeguards to ensure that data transfer occurs in adherence with data protection regulation.

**Will Sycamore Education notify users if a data breach has occurred?**

Depending on the nature of the data breach, our customers might be required to promptly notify both the users affected and the supervising authorities. Sycamore Education is required to notify its customers when becoming aware of a data breach, and to help them in fulfilling obligations in notifying users.

**Can I require a cloud service provider, like Sycamore Education, to only host personal data in my country?**

One of the GDPR's primary objectives is the free flow of personal data inside the European Economic Area (EEA), under one common regulation. In most cases, restricting vendors in processing data across the EEA would not be permitted under GDPR.

**Does Sycamore Education process data outside the EEA? Is it allowed to process data outside the EEA?**

GDPR does not forbid personal data to flow outside the EEA, but expects that any data processing outside the EEA is done following the same principles.

In addition, controllers or processors that process data outside the EEA must provide detailed information about the nature of the processing. In some cases, they must also allow customers or users to object to the processing..

**Does GDPR impact customers outside the EU?**

Not legally. The EU, obviously, has no legislative power over other jurisdictions. GDPR does not offer any rights or freedoms to data subjects located outside the EU, and does not put obligations on non-EU customers that do not process data on EU/EEA data subjects.

However, Sycamore Education offers, for the most part, the same services and same level of security to all our customers. In other words, no matter where your school is located, you will benefit from our approach to security of personal data under GDPR.

**Who do I contact with further questions?**

For general questions related to Sycamore Education you can always contact our support team at support@sycamoreleaf.com.

For specific GDPR-related questions from our customers, please contact our Data Protection Officer Karla Dorsey. In addition to monitoring our own compliance and providing advice and training to our own staff, our DPO will be available to our customers and their DPOs to discuss data privacy issues.

She can be reached at dpo@sycamoreleaf.com. Please note that any communication with our DPO must be in English.