White Paper - Privacy and Data Protection

Last updated: 9 November 2023

Introduction

At Kognity, we are committed to providing all students with modern and engaging high-quality learning experiences. This commitment is central to our vision of *radically improving learning for the world's 1.5 billion school students*. To achieve our goal, we understand the importance of trust in our relationships with students, teachers and partner schools. We deeply value the trust placed in us and are committed to upholding this responsibility by rigorously protecting personal data.

Our commitment to You

We are committed to protecting the personal data of our student and teacher users ("**Platform Data**"). Our respective responsibilities concerning Platform Data are set out in our Standard Subscription Agreement Terms and our Privacy Notice, as well as under applicable laws. Depending on Your jurisdiction, these may include the European Union's General Data Protection Regulation (GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) or the UK GDPR and Data Protection Act 2018.

Data privacy is in our DNA

Originating in Europe, we have a strong foundation in rigorous data protection practices. As we have expanded, our dedication to safeguarding Platform Data has been unwavering. The principles of data privacy are deeply embedded in our operations, ensuring that we meet the high expectations of our partners and users and comply with the stringent requirements of applicable data privacy laws.

The Platform Data are Your data

To be able to improve learning and shape the future of education, we need to receive and process certain Platform Data from You. The key point in this statement is that the data we collect and process remain Your data and You retain ownership over the Platform Data. Under regulations such as the GDPR, this is commonly referred to as You being the data controller while we are the data processor.

The Platform Data we will need to collect and process to deliver our services can be split into three categories (in addition to general device or usage data):

- *Onboarding data*: basic information about who is in the classroom and who teaches the class, including names, emails, year or graduation, subject and school
- *Product generated data*: platform data related to usage, including student progress, usage, results, assignments, assessments and progress and teacher comments and feedback
- *Account and support data*: basic information relating to a customer's account and personal information relating to customer inquiries or platform support matters

Our Standard Subscription Agreement Terms incorporate a data processing agreement that outlines how Platform Data will be handled and protected by us, as well as ensuring that we meet legal requirements.

How we use Your data and not

We will only use Your Platform Data to deliver and improve our services, provide related support and ensure secure and effective operation of the services. We will never sell any student Platform Data, use it for marketing purposes or for any commercial purposes other than those mentioned just above.

How we leverage third-party service providers

We are a cloud-first company meaning that we leverage cloud technologies to host and provide our platform. This means that we can deliver our service to You in a secure and effective way. It also means that we work with selected and trusted third-party service providers (so called subprocessors). For example in relation to hosting of our platform, in-app support functionality and to manage back-end systems. A list of these providers from time to time is available here, and we will of course notify You if we choose to add any subprocessors.

It goes without saying that we are responsible for their handling of Platform Data. We have implemented adequate oversight and contractual obligations with them to live up to the requirements of our privacy and information security program. Each provider must also continuously pass our rigorous vetting process. If any provider is located outside of the EU/EEA, we ensure that appropriate transfer safeguards are implemented. You can see what safeguards apply in the list mentioned above.

Data subject rights - we got You

As required by GDPR and similar laws, we have implemented procedures and processes to allow for our users to enjoy their data subject rights, including the right to access, correct, delete and restrict the processing of their Platform Data. As the Platform Data are Your data, however, we will ask You how You want us to proceed if we receive any requests directly from a user.

Data security is key

We firmly believe that protecting Your Platform Data begins with keeping the data secure. Hence, we deploy a comprehensive information security program to protect all aspects of Your Platform Data. The program is based on and aligns with the National Institute of Standard and Technology (NIST) Cybersecurity Framework, the International Organization for Standardization (ISO 27001), Service Organization Control (SOC 2) and IMS Global/1EdTech.

Our information security work is verified through our SOC 2 type I attestation, which is available on request subject to customary non-confidentiality underwriting. We are also in the process of obtaining a SOC 2 type 2 attestation, which we estimate will be available February 2024 at the latest.

Our Controls

Below is a selection of the controls we deploy. For more information on our controls and information security work, just ask us for our Data Security & Privacy Plan which we would be happy to share with You.

Encryption in rest and in transit
All Platform Data are subject to encryption both in transit and in rest

Continuous de-identification or deletion
Platform Data are continuously de-identified or deleted, for example when a student graduates or You decide to no longer use our services

Privacy by design
Privacy is an integral part of our engineering process as well as other processes (for example permission levels for data access)

Staff training
Mandatory and recurring trainings on information security and privacy guarantees awareness

Background checks
Criminal background checks are carried out in relation to all staff that may access Platform Data

Threat monitoring
Our security operations center and endpoint detection response tool allows us to continuously monitor any threat, exploit or vulnerability

Disaster recovery & backups
Platform Data are protected from loss through disaster recovery policies, including daily database backups

Secure passwords
For user access, multi-factor authentication and secure passwords are enforced

Questions?

We’re happy to share further insights into our privacy and data protection work. In the first instance, reach out to your Kognity contract person or email us at dataprotection@kognity.com.

We look forward to radically improving learning together with You!