anthology

How the Anthology Data Privacy Program Supports Our Clients

Prepared by the Anthology Privacy Team

Contents

Introduction

The data privacy[1] landscape around the world has changed significantly over the past years. From the adoption and entry into force of the EU General Data Protection Regulation (GDPR) to the most recent state consumer privacy laws in the U.S. to the Brazilian LGDP, a new generation of data privacy laws is covering the world with higher expectations on organizations and more power for regulators.

What hasn't changed is Anthology's commitment to high standards of data privacy. We understand that data privacy is a fundamental right for all individuals. That is why we used the implementation of the GDPR as an opportunity to apply the high EU standards globally.

Our clients entrust us with detailed information about their users/students. Our clients want to be sure that they can trust us with their data. It is our responsibility to demonstrate and earn that trust.

We take that responsibility seriously and are a signatory of the Student Privacy Pledge 2020, a member of the Future of Privacy Forum, and proud to have several products certified under ISO 27001, ISO 27017, and ISO 27018.

This white paper is designed to give our clients an overview of our Data Privacy Program, detailing our approach to upholding the different data privacy laws around the world and laying out how our efforts support their organizations and keep their data secure.

Anthology's Data Privacy Commitments

The following commitments form the basis of our Data Privacy Program. These commitments are reflected in our internal policies and in our contracts with our clients.

- **Our clients own their data.** We understand that the personal information[2] of our clients' users is only entrusted to us. We have a responsibility to protect it vigilantly and only use it in accordance with all applicable data privacy laws and with our contractual agreements with our clients.
- **We believe data privacy is a fundamental right for all individuals.** We made the decision early on to adopt the high EU GDPR standards globally.
- **We do not sell student data.** We do not sell student personal information to third parties or data brokers or use or disclose student personal information for targeted advertising purposes.
- **Innovation guided by privacy by design.** We help our clients with data-driven insights and personalization. Our privacy team works closely with our product teams on these innovations, and we apply a privacy-by-design approach.

Working with Our Clients to Protect Personal Information

Under the U.S. Family Educational Rights and Privacy Act (FERPA), the EU GDPR, and most other data privacy laws and regulations, we and our clients have defined roles and responsibilities. Our clients are generally responsible for determining what purposes personal information is used for, ensuring that they are allowed to collect and use personal information and are transparent about their use of personal information. Anthology, in turn, is responsible for adequately securing this data, supporting our clients with their own compliance obligations (e.g., conducting data privacy impact assessments), and only using this personal information as permitted in the contract. These roles and responsibilities are clearly defined in our contracts, and we understand the importance of supporting our clients with their data privacy responsibilities.

Our Data Privacy Program

To translate the commitments listed above into actions that support our clients, we have a dedicated Data Privacy Program that uses the high EU GDPR standards as a global baseline. This helps us to ensure we can meet our obligations and can assist our clients with their obligations worldwide. Core aspects of our program are our internal policies, our governance model, and our training and awareness activities.

Our internal data privacy policies define our principles, our governance model, and the requirements our products need to meet. Our policy principles are based on the principles of the EU GPDR, the U.S. Fair Information Practice Principles (FIPPs), and the principles of Convention 108. These principles apply globally

— both when we use personal information for our purposes (as a "controller") and when we use the personal information of our clients on their behalf (as a "processor").

Good data privacy practices require a solid governance model. At Anthology, data privacy and security are a board priority, and our data privacy governance model (see graphic below) ensures that senior management oversees and supports our data privacy and security efforts.

To further embed data privacy throughout the organization, we have a network of data privacy champions in every functional area and product group. The data privacy champions assist with spreading awareness and dissemination of information about our internal policies and guidance, escalating issues, and assisting their functional area with data privacy requirements and processes.

Board Level	**Board (Audit Committee)**	
	• Privacy and security are a board priority • Audit committee receives regular updates on compliance risk management, including privacy and security	
Senior Management Level	**Compliance Committee**	
	• Cross-functional oversight over compliance risks, including privacy and security • Senior management membership, including CEO, chief legal officer, CFO, compliance officer, CISO, and global privacy officer	
Management Level	**Security and Privacy Risk Council**	
	• Cross-functional council to manage and align data privacy and security programs and related risks, as well as tracking new legal requirements regarding data privacy and security • Functional leadership, including CISO (chair), global privacy officer, compliance officer, and head of vendor risk management, as well as representation from product teams	
Working Level	**System Security Officers**	**Data Privacy Champions**
	• Every product has a system security officer who is responsible for managing implementation of internal security programmatic controls	• Each product group and corporate function has a data privacy champion who is responsible for supporting the privacy program, privacy by design, and escalating issues

The importance that Anthology places on data privacy and security is also highlighted by the fact that our global privacy officer and chief information security officer report directly to the CEO Leadership Team.

To ensure staff awareness, Anthology has security and data privacy training that is rolled out to all staff when joining Anthology and on an annual basis. The data privacy training explains key legal frameworks (including EU GDPR, U.S. state privacy laws, and FERPA), concepts, and definitions. It also details Anthology's data privacy principles and Anthology's privacy governance. The security training provides guidance on Anthology's data sensitivity classifications, the protection of IT assets, securing the workspace, protection from phishing, and other key aspects of the Acceptable Use Policy. Additionally, Anthology conducts regular data privacy and security awareness activities.

Privacy by Design

Anthology is constantly looking to develop new products and functionalities. An important focus of our innovation is helping our clients with data-driven insights and personalization. To ensure that this innovation and data privacy go hand in hand, we implemented clearly defined data privacy requirements and have developed a documented privacy-by-design process. The data privacy requirements have been developed in cooperation with our product teams. They translate our data privacy commitments and principles as well as ISO 27018 controls into detailed and prescriptive product requirements. The data privacy requirements are supplemented by our privacy-by-design approach that formalizes the legal/privacy review of product development and product changes. The combination of the data privacy requirements and the privacy-by-design process helps ensure that material changes to the use of personal information take into account the data privacy rights of individuals and are built in a manner that minimizes the impact on the data privacy rights of individuals. It also means that new products and functionalities are developed in a way that allow Anthology to comply with applicable data privacy laws and support our clients with their data privacy obligations.

Contractual Commitments

We understand that robust data privacy clauses in contracts are, alone, not sufficient to meet privacy regulations, but these clauses translate our commitments and principles into legally binding obligations. Consequently, we use one global "data processing addendum" that provides the high GDPR standards to all our clients globally — regardless of the level of data privacy laws in their jurisdiction. The data processing addendums are also crucial in outlining how we support our clients with requests from individuals, data protection impact assessments, and audits. It also defines the limits of our data use and describes our security controls in detail. We regularly update our standard data processing addendum to ensure our clients can benefit from clauses that reflect the latest legal and regulatory changes.

Responsibility for Our Vendors

Most of our products and services rely on specialized vendors that support us in providing our products and services to our clients (e.g., hosting and monitoring application performance). We understand that we are responsible for the data privacy practices of these vendors ("subprocessors") when we allow them access to our clients' personal information. We, therefore, have set up a vendor risk management process. This process helps us ensure that we have a robust contract with a data processing addendum in place with our third-party vendors imposing materially equivalent provisions to the ones we have in place with our clients. In addition, vendors with access to our clients' personal information need to complete vendor security and data privacy due diligence questionnaires before the start of the engagement and regularly thereafter. This allows us to understand their security and privacy practices and make sure they meet our standards. Also, vendors with access to Anthology-managed systems are required to follow Anthology-internal access control and identity and authorization policies, which includes that they need to access Anthology resources through approved mechanisms.

Keeping Personal Information Secure

An important aspect of data privacy compliance is protecting personal information with technical and organizational measures that are commercially reasonable and appropriate to the risk posed by the nature, scope, context, and purpose of the use of personal information. Our security program and policies are closely aligned with the ISO 27000 family of standards as well as NIST 800-53. As mentioned above, we detail these security measures in our data processing addendum. We have also achieved ISO 27001/27017/27018 certifications for key products and SOC 2 for our **Anthology® Student** and **Anthology® Reach** products.

To help our clients with their security due diligence, we provide copies of our certifications and SOC reports, as well as our responses to the **Higher Education Community Vendor Assessment Toolkit (HECVAT)** questionnaires, which are frequently updated to reflect our most current practices, upon request.

You can find more information in our **Product Security Statement**.

Data Hosting and Transfers

Many Anthology products are regionally hosted. Access from outside the hosting location may be necessary for 24/7 client support, product maintenance purposes, and additional functionalities. Any access only takes place on a need-to-know basis.

To ensure that client/student data receives a high level of protection when it is accessed from outside the hosting locations, we use the 2021 Processor-to-Processor EU Commission Standard Contractual Clauses (P2P SCCs) that are incorporated within Anthology's group of companies through intra-group data transfer agreements. In May 2019, we also submitted our Binding Corporate Rules (for processors) for authorization and will mainly rely on the Binding Corporate Rules for transferred EU personal information once authorized.

Further measures to protect transferred personal information:

- When data is transferred via the internet, it is encrypted in transit
- Client data is encrypted at rest
- Employees only have access to the personal information they need for the performance of their role (least-privilege principle)
- Employees must use multi-factor authentication for remote access to the IT infrastructure
- A select number of products are ISO 27001 and ISO 27018 certified
- Detailed contractual commitments regarding the level of security controls
- Contractual commitments on how we protect personal information of our clients in the case of requests by foreign authorities

For our EU/EEA/UK clients, we have also conducted a transfer impact assessment based on the "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data" by the European Data Protection Board (EDPB recommendations), which is available upon request.

Keeping Up with Data Privacy Laws Around the World

Data privacy laws and regulations across the world continue to evolve and mature. We are therefore constantly on the lookout for any new legal requirements that are applicable to us or our clients. Anthology's privacy team, with the help of a network of local law firms, is permanently monitoring and tracking regulatory updates and changes. Moreover, we are a member of the Future of Privacy Forum (FPF), an organization that is constantly updating its members on legal changes being discussed, introduced, and adopted around the world. The Anthology privacy team consolidates and tracks these external updates in our global law monitoring and implementation tracker.

Once a change to data privacy laws has been adopted, we will review the changes to determine if we need to make any revisions to our data privacy setup. Using the EU GDPR as our global standard helps us meet most changes to local data privacy laws. However, we understand that local laws may vary from GDPR and hence may require changes to our client and vendor contracts, our internal Data Privacy Program processes and documentation, our external privacy statements, or our products. Where such changes are necessary, we implement them through dedicated implementation projects. For instance, in the last few years, we made specific changes to address the requirements of GDPR, the California Consumer Privacy Act (CPRA), recently enacted U.S. State Laws (Colorado, Connecticut, Nevada, Utah, and Virginia), the South African Protection of Personal Information Act (POPI Act), and the Brazilian General Personal Data Protection Law (LGPD).

Trustworthy AI

As Artificial Intelligence (AI) increasingly becomes part of our day-to-day life and helps Anthology deliver more data-driven insights and personalization in our products, Anthology is responsible for using AI in an ethical and legal manner that respects the fundamental rights of individuals and addresses AI risks.

To formalize our approach, we are working on a Trustworthy AI framework that will define our principles, formalize the review process, and include training and guidance for our teams working with AI. Our Trustworthy AI framework will be aligned to existing frameworks for the ethical use of AI and upcoming legislation such as the **OECD AI principles**, the draft **NIST AI Risk Management Framework**, and the draft EU AI Act. It will be based on principles such as fairness, robustness, explainability/transparency, accountability as well as privacy, security, and safety.

Footnotes

[1] While the concept and terminology vary across the globe (with European clients more familiar with the term "data protection"), we use the term "data privacy" to refer to the fundamental rights of individuals and the corresponding obligations of organizations in relation to the use of personal information.

[2] We use "personal information" interchangeably with "personal data" to mean the information relating to an identified or identifiable individual.

Additional Resources

You can find more information in the **Anthology Trust Center** and the Anthology Community on our **Privacy & Security page**.

If you have any questions or feedback regarding this white paper, please contact us at **privacy@anthology.com**.

Disclaimer

These materials have been prepared for informational purposes only and are not legal advice. Please seek the advice of your privacy/legal team for any questions about the application of data privacy laws.

About Anthology

Anthology offers the largest EdTech ecosystem on a global scale, supporting over 150 million users in 80 countries. The company's mission is to provide dynamic, data-informed experiences to the global education community so that learners and educators can achieve their goals.

Through Anthology Intelligent Experiences™ and over 60 SaaS products and services, Anthology advances learning in partnership with education, business and government institutions. Tapping into this unmatched portfolio of solutions, only Anthology can leverage data from across the EdTech ecosystem to create Intelligent Experiences that lead to better outcomes.

Learn more about our mission at **www.anthology.com**