

Integrity Advocate & GDPR

Introduction:

On May 25th, 2018, online educational services, even those outside the European Union (EU), became accountable for all their data under the EU General Data Protection Regulation (GDPR). This regulation is designed to protect all EU citizens' data privacy and to harmonize all data privacy laws across Europe. GDPR affects what data can be collected, how it can be used, where it can be stored, and how long it can be stored.

Online education services are challenged with providing a participation monitoring and proctoring service that not only enables the best possible user experience and robust integrity controls, but also adheres with the required privacy protection for learners. GDPR has created a uniform European legal framework that now gives subjects who reside in Europe rights over their data.

Purpose & Scope of GDPR

GDPR safeguards the protection of natural persons (individual people) when their personal data are processed and provides rules on the free movement of personal data. The regulation seeks to protect fundamental rights and freedoms of natural persons and, more specifically, their right to the protection of personal data. GDPR does not govern the rights and freedoms of legal persons, including companies.

GDPR applies if the organization that collects data or processes data or the data subject (person) is based in the EU. This applies to all organizations, regardless of whether they are based in the EU or not.

According to the European Commission, "Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address."





Why does this matter?

The impact of GDPR on online educational services has been notable. Proctoring services are now under pressure to become more accountable for the data they possess and share. Their records must be organized in terms of what personal data exists, as well as documentation explaining why it has been held, how it was collated, who has access to it and when it will be removed or anonymized.

It is more important than ever that service providers ensure measures are in place to keep personal information secure. Any breaches must be reported to the ICO within 72 hours and must be reported to the individual whose data has been compromised if the breach relates to identity or financial theft.

There is an emphasis on “data protection by design”; new information handling systems and processes must be developed in accordance with new guidelines outlined by GDPR. In short, personal data must be protected from the very beginning of a product lifecycle.

Consent to use personal data has been redefined and refined. Online educational services must now be able to evidence that consent to use information was “freely given, specific, informed and unambiguous”.

As our expectations for data protection have risen, so have the consequences for non-compliance. Those who do not comply can now face fines measured in a percentage of annual turnover.

Framework for Compliance

The GDPR sets out seven key principles that have a direct application to the online education space:

- Lawfulness, fairness, and transparency
- Purpose limitation
- Data minimization
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

GDPR Article	Requirement	How Integrity Advocate Complies
Article 5(1)(a)	“processed lawfully, fairly and in a transparent manner in relation to individuals (‘lawfulness, fairness and transparency’);”	By design, Integrity Advocate has made protecting learner privacy the end-goal of its operations while making a concerted effort to inform users and institutions alike what data is lawfully being collected, what may be shared, and what needs to be deleted.
Article 5(1)(b)	“collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘purpose limitation’);”	Integrity Advocate not only restricts the processing of learner information to its stated purpose of verifying identity and participation in client rules, but also acts as an intermediary and protects the redistribution of personal data where not necessary to support incidents of non-compliance.
Article 5(1)(c)	“adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’);”	Integrity Advocate has data minimization options that eliminate the need for ID resubmissions where the learner’s image was previously validated and has developed a process that deletes all unnecessary data, including government issued ID’s (where used) within 24 hours of submission.
Article 5(1)(d)	“accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);”	Integrity advocate provides all users with a copy of retained data, our review findings and reviewer notes to allow them to verify data accuracy and the conclusions drawn from the processing of their data.
Article 5(1)(e)	“kept 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organizational measures required by the GDPR in order to safeguard the rights and freedoms of individuals (‘storage limitation’);”	Integrity Advocate deletes all unnecessary data i.e., data not required to illustrate who participated in the event and/or to support any rule violations identified. The limited data retained is deleted after 24 months, unless otherwise stipulated based on a client/regulatory requirement.
Article 5(1)(f)	“processed 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 (‘integrity and confidentiality’).”	Integrity Advocate encrypts user data in-transit and at rest, completes all possible data processing on the user’s device (minimizing on-line traffic), as well as retains the data of UK residents within the UK or on servers within Canada (based on client preference).



Conclusion

Online education services are challenged with providing a participation monitoring and proctoring service that not only incorporates the best possible user experience with robust integrity controls, but also adheres to the required privacy protection for learners. Integrity Advocate has demonstrated compliance with GDPR and allows for institutions to utilize our services with confidence that the intent of GDPR - the **right to the protection of personal data** - has been met.

Corporate Headquarters: 13A Perron Street, Saint Albert Alberta, T8N 1N2

2020 Integrity Advocate Inc. All rights reserved. Integrity Advocate, the Integrity Advocate logo and other marks appearing here are the property of Integrity Advocate Inc. All other marks are the property of the respective owner(s).

www.integrityadvocate.com

Customer Service Support: +1 (888) 395-1025

CSR Management: United States: +1 (650) 665-6993 | Australia: +61 2 4050 0222 | United Kingdom: +44 20 8103 9092 | Canada: +1 (226) 407-6583