

## The National Student Clearinghouse’s Collaborative Approach to GDPR Compliance

The European Union’s General Data Protection Regulation (“GDPR”) protects the privacy and security of personal data collected from individuals within the territory of the European Union (“EU Data Subjects”). It applies to organizations established outside of the EU if they: (i) process the personal data of EU Data Subjects when offering them goods or services; or (ii) monitor the behavior of EU Data Subjects. The Clearinghouse neither offers goods or services to EU Data Subjects nor monitors their behavior - therefore, the GDPR does not apply directly to the Clearinghouse. However, the Clearinghouse works with organizations that collect or process the personal data of EU Data Subjects and who are therefore directly subject to the GDPR. These organizations must ensure that any processing of personal data of EU Data Subjects they collect is compliant with the GDPR (including processing by other parties that receive the personal data), and the Clearinghouse provides the following collaborative approach to help these organizations achieve GDPR compliance for any processing activities performed by the Clearinghouse:

When a customer uses a Clearinghouse service to process personal data, the Clearinghouse is processing on behalf of and at the direction of the customer. The customer must ensure that the purpose and means of processing complies with the data protection principles of the GDPR (including, among others, that (1) personal data may not be processed in any manner incompatible with the purpose for which it was collected and (2) the processing of personal data must be lawful) and that the purpose and means is accurately stated in the relevant service agreement it enters into with the Clearinghouse. The customer is also required to enter into a contract (a “Data Protection Addendum”) with the Clearinghouse that imposes certain obligations required by the GDPR under Article 28. And, because the Clearinghouse is a data processor located outside of the European Union, the transfer of personal data to the Clearinghouse is required to have safeguards deemed adequate under the GDPR’s Article 46. The Clearinghouse has prepared a Data Protection Addendum pertaining to each of our services that contains both the required obligations of Article 28 and the adequate safeguards of Article 46 of the GDPR. To request a copy of the Clearinghouse’s Data Protection Addendum, please email [privacy@studentclearinghouse.org](mailto:privacy@studentclearinghouse.org).

Article	Requirement	Clearinghouse’s Collaborative Approach
28	Processor guarantees	The Clearinghouse provides these guarantees through the Data Protection Addendum it enters into with customers that use its service(s) to process personal data of EU Data Subjects.
29	No incompatible processing	The Clearinghouse only processes personal data according to the directions provided by the customer in the applicable service contract. The Data Protection Addendum restates this restriction.
32	Security of Processing	The Clearinghouse maintains appropriate technical and organizational security measures to provide a level of security appropriate to the risks that are presented by the processing and the nature of the personal data to be protected.
33	Data breach notification	The Clearinghouse’s Data Protection Addendum commits the Clearinghouse to report any breach to the customer without undue delay after it becomes aware.