Pearson Education Transfer Impact Assessment - United States of America

Last reviewed in October 2021

On July 16, 2020, the Court of Justice of the European Union ("CJEU") issued its ruling in the case of the Irish Data Protection Commissioner v Facebook Ireland and Maximillian Schrems (Case C-311/18) ("Schrems II").

The ruling invalidated reliance on the EU-US Privacy Shield Framework as a lawful means to transfer personal data from the European Economic Area ("EEA") to the United States, while also affirming the EU Standard Contractual Clauses ("SCCs") as a valid data transfer solution.

This is a living document and Pearson will continue to update it. The document has been prepared for Pearson's customers and other stakeholders to help explain Pearson's approach to the protection of personal information pursuant to the Schrems II decision.

This document may be particularly helpful to customers who need to perform their own data transfer impact assessment pursuant to the Schrems II decision. This document does not form a part of any contractual document or agreement. It is provided solely as a source of information and customers should make their own determinations and, if necessary, seek independent legal advice.

Overview of the Data being Transferred	
Description of the Transfer	Pearson Education Inc, its affiliates, and subsidiaries ('**Pearson**') processes customer personal information in order to provide the educational and assessment products purchased by customers ('the **Services**')
Safeguards relied upon to protect the data being transferred	The Standard Contractual Clauses published by the European Commission.
Describe the data being transferred and the reasons for it.	The processing activities for the Services include the delivery of course content, assessments and educational activities chosen by institutions or individual consumers and the storage of that information together with related account configuration, maintenance ,in-app activity and customer and business support activities.
Categories of personal information being transferred	**Account Registration data**: Limited personal information is collected during the registration process for the Services. This normally includes First Name, Last Name and email address. In addition, where relevant, we may also collect a learner's institution and course identifier. Personal information for institutional account administrators will also include their job title and the billing address for that institutional customer. **User Generated data**: As users of the Services, learners and instructors/admninistrators may also generate personal information when using the Services, including assignments, student coursework,

	responses to interactive exercises, scores, grades and instructor comments. **Service Generated data**: Device and product useage data which is collected or generated in the course of a user interacting with the Services. None of the information collected or generated by the Services is likely to be of interest to government or surveillance activities and it does not include social media content or other material shared or created in forums or discussion groups. This information is described in more detail in Pearson's Digital Learning Services Privacy Notice.
The recipients of the personal information	Pearson is the recipient of the personal information. A list of the third party suppliers and sub-processors whom Pearson relies upon to provide its services is available from your Pearson representative (this list varies by product).
Why must this personal information be processed outside of the UK/European Economic Area?	The Services are designed in and supported from the United States and, in addition to ensuring that customers can benefit from 24/7/365 support, Pearson may need to store personal information in or access it from the United States in order to ensure that the Services can be delivered.
B. Regulatory Framework	
Is the recipient in the UK or EEA?	No. Pearson is located in the United States of America and third part sub-processors may also be located outside the UK/EEA.
Has the recipient country implemented legislation or executive powers which could affect Pearson's ability to comply with its obligations under applicable data protection legislation?	Yes • **Pursuant to s. 702 FISA**, the United States government ("**USG**") can compel "electronic communications service providers" to disclose information about non-US persons located outside the US for the purposes of foreign intelligence information gathering. This information gathering is jointly authorised by the US Attorney General and the Director of National Intelligence, and must be approved by the Foreign Intelligence Surveillance Court in Washington, DC. Once approved, USG sends relevant providers certain "selectors" (such as telephone numbers or email addresses) associated with specific "targets" (such as a non-US person or legal entity). In-scope providers must comply with these directives in secret and are not allowed to notify their users. In-scope providers are electronic communication service providers (**"ECSP"**) within 50 U.S.C § 1881(b)(4), namely: electronic communication service providers (**"ECS"**) and remote computing service providers (**"RCS"**), as defined under 18 U.S.C. § 2510 and 18 U.S.C. § 2711; a

	telecommunications carrier, as defined in 47 U.S.C. §153 – i.e., a provider that has traffic flowing through its internet backbone and that carries traffic for third parties other than its own customers; any other communication service provider who has access to wire or electronic communications either as such communications are transmitted or as such communications are stored; and any other relevant U.S. entity that is an officer, employee, or agent of one of the entities described above. • **Pursuant to Executive Order 12333 ("EO12333")**, USG authorises intelligence agencies (like the US National Security Agency) to conduct surveillance outside of the US. In particular, it provides authority for US intelligence agencies collect foreign "signals intelligence" information, being information collected from communications and other data passed or accessible by radio, wire and other electromagnetic means. This may include accessing underwater cables carrying Internet data in transit to the United States. EO12333 does not rely on the compelled assistance of service providers, but instead appears to rely on exploiting vulnerabilities in telecommunications infrastructure. • **Pursuant to the Electronic Communications Privacy Act ("ECPA")**, all ECS and RCS may or must disclose user/subscriber records and communications, both to law enforcement and private parties. Generally, ECPA restricts when ECS and RCS can freely disclose information. Communications content (email, private messages, photographs, etc.) is generally subject to the strictest rules, and "basic" subscriber information (name of account holder, types of service they receive, etc.) are provided the least protection. An ECS/RCS can be subject to various types of legal process (subpoena, 2. 18 U.S.C. 2703(d) court order, court-issued ECPA warrant, pen register and trap and trace court order and court-issued Title III Wiretap), each of which is either issued by a court or otherwise subject to judicial oversight. An ECS or RCS may be compelled to produce data to U.S. law enforcement for criminal investigative purposes if such data is within its possession, custody, or control regardless of whether such data is stored within or outside of the United States and often regardless of whether the ECS or RCS itself is in physical possession of the data. • **National Security Letters ("NSLs")** can be issued without judicial oversight under ECPA, the Fair

	Credit Reporting Act, and the Right to Financial Privacy Act. The USG must certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.
Is Pearson potentially within the scope of the legislation and powers described above?	Not directly. Pearson is not an ECSP, ECS or RCS as define above however as a US business Pearson inevitably relies upon sub-processors who are governed by the legislation in question. Moreover, there is a possibility that personal information transmitted to or from Pearson will be accessed by the United States government acting in accordance with EO 12333. For the sake of clarity and avoidance of doubt, Pearson does not and has not provided the US government with any information or assistance in connection with EO123333 and it does not permit the creation or use of vulnerabilities in its infrastructure which might support such activity. As a result, Pearson has implemented the supplementary measures referred to below in order to address the potential gaps in the protection afforded to personal information which is transferred to it.
C. Assessment of Recipient's Safeguards	
Has Pearson ever received any requests for access to data from public authorities in the United States for access to personal information relating to personal information from the UK or EEA and that it is not prohibited from providing information about such requests or their absence.	Pearson has never received an order to disclose personal information from the EEA or UK to US government agencies. This reflects the fact that the personal information processed by Pearson is unlikely to be of use to such government agencies for the prevention and detection of criminal activity or other unlawful behaviors.
Could Pearson be subject to a request for access to personal information in the UK or EEA under FISA?	No. Pearson is not subject to FISA as it is not an ECSP, ECS or RCS for the purposes of that legislation.
Is Pearson subject to EO 123333?	Pearson does not voluntarily provide information or assistance in connection with EO123333 and EO 12333 cannot be used to compel Pearson to provide any such assistance.
Does Pearson have policies organizational methods or standards in place which apply to the transfer of personal information and access to transferred information by third parties?	Yes. Adequate internal policies exist with clear allocation of responsibilities for data transfers, reporting channels and standard operating procedures for formal or informal requests to access the data (especially for intragroup transfers), including appointment of a specific team (IT, data protection and privacy experts) to deal with requests that involve personal data transferred from the UK/EEA; notification to senior legal and corporate management upon receipt of such requests; procedural steps to

	challenge disproportionate or unlawful requests; and provision of transparent information to data subjects. Training is in place for personnel in charge of managing requests for access, periodically updated to reflect new legal developments in the United States, UK and EEA, including on EU and UK requirements as to access by public authorities to personal data, in particular Article 52 (1) Charter of Fundamental Rights, raising awareness of personnel by assessment of practical examples of public authorities' data access requests and by applying the Article 52(1) standard to the practical examples, taking into account local legislation and regulations
Does Pearson maintain transparency and accountability measures regarding public authorities access to personal information?	Yes. Pearson documents and records requests and responses for all access requests whatever the source. However, Pearson has no information to disclose regarding US government requests as it has never received any and has not been obliged to keep any such requests confidential.
Will Pearson notify customers about any government request for access to personal information?	Yes. Pearson will notify any Customer whose personal information is affected by such a request unless expressly prohibited from doing so by applicable law.
Does Pearson pseudonymise personal information before it is transferred?	Yes. Even though Pearson products and platforms may be supported from the United States Pearson seeks to localize personal information by default so that personally identifiable information is stored in the UK and/or EEA. Pearson's identity management systems used for accessing digital products have been designed to store personally identifiable information in the region from which it originates, whilst data relating to the usage of platforms, which on its own cannot be used to identify users, is stored in the United States and in other countries. Disclosure or unauthorized use of the information needed to identify specific users is prevented by appropriate organizational and technical safeguards, including the implementation of least privilege access controls, training for all employees on the handling of personal information and in particular on dealing with requests for access to personal information.
D. Security Measures & Additional Safeguards	
What security measures does Pearson have in place to mitigate the risk associated with transferring personal information outside the UK and EEA?	All personal information is encrypted at rest and in transit using state-of-the-art encryption algorithms which are implemented using software without known vulnerabilities.

	Transport encryption is used with state-of-the-art encryption protocols to provide effective protection against active and passive attacks with resources known to be available to the public authorities Specific protective state-of-the-art measures are used against active and passive attacks on sending and receiving systems providing transport encryption, including tests for software vulnerabilities and possible backdoors.
What other security measures are in place?	A detailed description of the security measures used to protect personal information is contained in Pearson's General Security Overview.
Has Pearson implemented confidentiality, audit and escalation measures governing transfers of, and access to, data	Yes. Pearson has in place strict and granular data access and confidentiality policies and best practices, based on a strict need-to-know principle, monitored with regular audits and enforced through disciplinary measures, focusing on data minimisation with technical measures to restrict access (it might not be necessary to transfer certain data e.g., restricting remote access to EEA data for support, or when service provision only requires transfer of a limited dataset and not the entire database). Pearson has also engaged in the development of best practices to appropriately and timely involve and provide access to information to the data protection officer and to legal and internal auditing services on matters related to international transfers of personal data, before transfers are effected
Is there evidence of adoption of standards and best practices by group companies importing personal information?	Yes. Pearson has in place strict data security and data privacy policies, based on EU certification or codes of conducts or on international standards (e.g. ISO norms) and best practices (e.g., ENISA) with due regard to the state of the art, in accordance with the risk of the categories of data processed. Pearson has adopted and regularly reviews internal policies to assess suitability of implemented complementary measures and identify and implement additional or alternative solutions when necessary, to ensure that an essentially equivalent level of protection is maintained. Pearson group companies have also provided commitments not to engage in any onward transfer of the personal data within the same or other third countries, or suspend ongoing transfers, when an essentially equivalent level of protection cannot be guaranteed.

E. Overall Risk Assessment	
Assessment of the risk associated with this transfer	In view of the assessments of the group structure, the location of group companies in the United States, the data transferred, and the appropriate safeguards implemented by the group, the risk of proceeding with the intra-group transfers is modest and the transfers should be permitted to proceed.
Risk mitigations measures recommended prior to transfer:	Apart from the privacy requirements outlined in the intra-group agreement to secure data in the data, privacy impact assessments are performed by Pearson's Data Privacy Office prior to transfers being carried out and to review alternatives to data transfers wherever possible.