Frequently asked questions about personal data management and Privacy Shield

Clara Hardarsson - 2025-09-10 - Manage data and security

How does Skolon ensure our sub-processors meet security requirements under the GDPR?
Skolon places high demands on its **sub-processors** and their handling of personal data. The sub-processors' commitments to Skolon, regarding the processing of personal data, are regulated in **data processing agreements (DPAs)**. These DPAs are designed in accordance with the requirements of **GDPR Article 28**, which includes demands for the sub-processor to implement necessary technical and organisational measures to ensure an appropriate level of security, in line with the requirements of Article 32.

Skolon uses a small number of carefully selected sub-processors. All of these are internationally recognised, reputable companies with high standards for security and integrity. Several of our sub-processors are certified with standards like **ISO/IEC 27001, 27017, 27018, and/or SOC 1/2/3**.

How does Skolon ensure that no personal data will be processed by any of the sub-processors' US-based functions?
Processing and storage of personal data handled by Skolon's US-based sub-processors takes place on servers located within the EU*. Our sub-processors are not permitted to transfer personal data to countries outside the EU/EEA except in strict exceptional cases. This might include instances where it's absolutely necessary for a sub-processor to deliver their services, or as a result of a compulsory request from an authority or court. When transferring personal data to a third country, such as the USA, appropriate safeguards (preferably **Standard Contractual Clauses**) are always used in accordance with the requirements of **GDPR Articles 44-50**.

*Excluding The Rocket Science Group, provider of the Mailchimp service.

How does Skolon ensure that sub-processors storing personal data in the USA meet security requirements under the GDPR?
Skolon applies the same high standards to its sub-processors regardless of where they are based or where personal data is stored. Even if a sub-processor stores personal data in the USA, the **GDPR** still applies, and its requirements and rules are in force.

The sub-processors' commitments to Skolon, concerning the processing of personal data, are regulated in **data processing agreements (DPAs)**. These are designed in accordance with the requirements of **GDPR Article 28**, which notably includes demands for the sub-processor to implement necessary technical and organisational measures to ensure an

appropriate level of security, in line with the requirements of Article 32. Skolon uses a small number of carefully selected sub-processors, all of whom are internationally recognised, reputable companies with high standards for security and integrity.

The transfer of personal data from the EU to the USA is supported by **Standard Contractual Clauses (SCCs)**. Following the ruling in the **Schrems II case**, it's no longer permissible to transfer personal data to the USA based solely on Privacy Shield. However, the same ruling highlighted that transfers supported by SCCs generally provide a satisfactory level of protection, and SCCs are considered an appropriate safeguard under **Article 46.2 (c)**. Skolon has therefore entered into supplementary agreements containing SCCs with all sub-processors where personal data transfer/processing occurs in the USA.

The EU Court of Justice stated in the Schrems II case that SCCs may, in some cases, need to be supplemented with additional safeguards if necessary to ensure a satisfactory level of security. However, the Court did not specify what these additional safeguards might be. Skolon is currently awaiting further guidance from the European Data Protection Board (EDPB) and will act accordingly.

If you have more questions or concerns about how Skolon processes personal data, please contact us at **support@skolon.com**.