

Schrems II Compliance Information

Version 1.0.0

This document explains Civilized Discourse Construction Kit, Inc.'s approach to lawful transfer of personal data to the United States jurisdiction under chapter 5 of the European Union General Data Protection Regulation after the Schrems II decision, which invalidated the US-EU Privacy Shield program.

Company and Service in Brief

CDCK hosts Internet discussion forums for customers. By their nature, those forums must process data that may relate to identified or identifiable people, such as user profile page information, discussion topic messages, and user-to-user messages. As websites, those forums also collect data on forum visitors that correspond to identifiers like Internet Protocol addresses, such as Web traffic logs.

Civilized Discourse Construction Kit, Inc. is a corporation formed under the laws of the State of Delaware. It is therefore subject to Delaware state law and United States federal law.

Operationally, CDCK is a fully “remote” company without any physical office. CDCK personnel include employees and independent contractors around the world, including in the United States. To host forums, CDCK personnel, including personnel in the United States, need access to forum computer systems and data in order to operate the forums, monitor them, respond to security concerns, field technical support requests, and so on, across a broad swathe of timezones.

CDCK uses a variety of third-party service providers to host forums, including data center operators like Equinix and cloud services companies like Amazon Web Services. Up-to-date details on our subprocessors, their processing, and their jurisdictions are available at discourse.org/subprocessors.

Transfer Mechanism

CDCK relies on the European Commission's updated Standard Contractual Clauses to transfer personal data out of the European Economic Area by incorporating them by reference into comprehensive data protection addenda.

Laws of Concern

Because national security and surveillance laws may conflict with European data protection rules, CDCK continually reassesses the practical reach of these laws to ensure our data transfers are adequately safeguarded.

CDCK is very likely subject to section 702 of the Foreign Intelligence Surveillance Act in the United States, a law that the European Court of Justice found inadequately protects the rights and freedoms of data subjects.

CDCK has never received any order or request for personal data, under FISA 702 or any similar national security or surveillance law of any other country. Neither

is CDCK subject to any court order or legal obligation that would prevent it from disclosing the existence or non-existence of such an order or request.

Risk Assessment

Many of our customers use the forums we host for them as public discussion forums. For example, many of our customers use their forums to host discussions among users of their products and services. The vast majority of messages on public forums, and therefore the vast majority of personal data processed by us for those forums, are published on the open World Wide Web without any access restriction. The risk to such personal data under laws of concern is minimal or nonexistent, since the data are available to anyone with an Internet connection, including United States government agencies and personnel, in any event.

The risk to non-public personal forum data, such as private user-to-user messages and nonpublic data about user accounts, likely correlates strongly with government interest in the subject matter of discussions the forum tends to host and in the people who chose to visit the forum and create accounts. For the overwhelming majority of our customers, who use their forums for discussions of their commercial products and services, or among common-interest communities, the level of government interest is very likely low or nonexistent.

Similarly, the risk to non-public data processed by private, internal, and otherwise access-restricted forums likely also correlates strongly with government interest in the subject matter of discussion on the forum. On occasion, potential customers express particular concerns that the kinds of discussions they intend to host on their forums might be more likely to attract requests under FISA 702. If you believe this may be the case with your company's forum, please notify your CDCK Community Team contact immediately.

Enterprise Discourse hosting deals on CDCK's standard terms document the intended use case for the forum near the beginning of the first statement of work for forum hosting.

Supplementary Measures

CDCK has adopted a policy for how we will respond to orders and requests under FISA 702 and similar national security laws, in case we ever receive such a request. CDCK's policy includes suspending processing, notifying our customer, minimizing disclosure, and resisting disclosure of personal data, in each case to the furthest extent permitted by law.

Since the Schrems II decision, CDCK has made available a broader choice of subprocessors and subprocessor locations, including data centers, cloud infrastructure zones, and content delivery networks within the European Union. While locating data within the European Union would not prevent a binding order under United States law from applying to United States personnel with remote access to those systems, it may help to reduce exposure of forum personal data to mass data collection systems applied to data in transit or at rest within jurisdictions like the United States.

In furtherance of compliance with SOC 2 Type II, ISO/IEC 27001:2013, and its

own internal policies, CDCK has established access and other controls to limit the CDCK personnel with access to personal data related to forums that we host for customers. These controls further reduce the number of CDCK personnel subject to United States jurisdiction with the ability to access personal data related to customer forums.

Contact

Please direct further privacy-related inquiries to privacy@discourse.org.