



Our purpose is people

UKG Inc. Schrems II Statement

Review Date: March 14, 2022

In the [Schrems II decision](#), the European Court invalidated the Privacy Shield, but concluded that transfers of personal data outside of the EEA are not illegal. Subsequently, the European Data Protection Board (EDPB) adopted a [final version of the Recommendations on supplementary measures](#), which are intended to help businesses better understand their obligation to implement appropriate supplementary measures to ensure an essentially equivalent level of protection for transfers of personal data outside of the EEA.

We transfer personal data from the EU to the US, India, and other locations to deliver security, support, billing, and other services to our customers. We have and will continue to rely on Standard Contractual Clauses (SCCs) in our data protection agreements for both intra-company data transfers and in agreements with our partners and vendors.

We have further reviewed the safeguards we have in place following Schrems II and can confirm that:

- UKG is not an “electronic communications service provider” under the applicable law and therefor is not subject to access requests under FISA 702 or Executive Order 12333.
- Generally, a customer uses our products and services to process personal information concerning their workforce. We believe our customers should control the information that they collect, create, communicate and store about their workforce. As such, we do not give anyone access to a customer’s information unless the customer instructs us to do so, consents, or we are legally obligated to do so.
- We do not support “back door” direct access to our operations (including our data stores) by any government or third party.
- We do not share our encryption keys or provide the ability to break our encryption keys to any government or unauthorized third party.
- We encrypt personal information when it is stored and while it is transmitted in our products and services. We limit access to and encrypt our encryption keys. We do not support a “Bring Your Own Keys” option for customers.
- Depending on the application in use by the customer, we maintain ISO 27001, ISO 27017 and ISO 27018 certifications, and SOC 1 and SOC 2 reports, which are available upon request, and under appropriate confidentiality provisions.

For more information regarding our technical and organizational measures, contact your UKG representative to obtain due diligence package for our product(s) and services(s).

Based on the information in this Statement, we have determined that we can proceed with the transfer of EEA personal data to countries outside of the EEA. UKG's transfers of EEA personal data to countries outside of the EEA are subject to the SCCs, which impose obligations intended to ensure EEA personal data transferred to countries outside of the EEA is afforded a level of protection that is essentially equivalent to that guaranteed by the data protection laws of the EEA and/or the United Kingdom.