Data Privacy Framework Statement

September 7, 2023

In the Schrems II judgement, the European Court invalidated the Privacy Shield, but transfers of personal data outside of the European Economic Area were, however, not illegal. Controllers and processors acting as data exporters were required to identify and implement appropriate supplementary measures to ensure an essentially equivalent level of protection to the personal data they transfer to third countries, Standard Contractual Clauses being one of these measures.

With the European Union passing an adequacy decision and allowing a new E.U.-U.S. Data Privacy Framework (DPF), UKG is now a certified organization under the framework. This change provides additional reassurances related to cross-border transfers of personal data from the European Union to participating companies in the United States, ensuring compliance with E.U. data protection laws.

As part of its provision of goods and services to customers, UKG carries out cross-border transfers of data from its EU subsidiaries to the US, India, and other locations for service provisioning. In addition, to ensure 24/7 support, UKG has implemented "follow the sun" support operations, with support and cloud monitoring teams in various locations worldwide, including the US and India.

UKG has historically relied and currently relies on EU Standard Contractual Clauses as the cross-border transfer mechanism for EU data as part of its intragroup data transfer agreements. UKG has also incorporated EU Standard Contractual Clauses as part of its data processing agreements and data sharing agreements with its customers, partners, and its vendors.

UKG, including all U.S. affiliates (UKG Inc., Kronos Incorporated, Kronos SaasHR, and PeopleDoc) complies with:

- The EU-U.S. Data Privacy Framework
- The Swiss-U.S. Data Privacy Framework
- The UK-US Data Privacy Framework

UKG has certified to the Department of Commerce that it adheres to the Data Privacy Framework Principles with respect to personal data transferred from the European Union, the UK, and Switzerland. Additionally, UKG has updated its privacy notice to align with the Data Privacy Framework Principles.

UKG has reviewed the safeguards it has in place regarding data transfers outside the EU. As such, UKG confirms that:

- Generally, a customer uses UKG products and services to process personal information concerning their workforce. UKG believes that a customer should control the information that they collect, create, communicate, and store about their workforce. As such, UKG does not give anyone access to customer information unless the customer instructs us to do so, consents, or we are legally obligated to do so.

- UKG does not support "back door" direct access to our operations (including our data stores) by any government.

- UKG does not share its encryption keys or provide the ability to break its encryption keys to any government.

- UKG does not voluntarily permit US or other governmental agency access to its infrastructure.

- As a Processor, UKG encrypts personal information when stored and while it is transmitted. UKG limits access to and encrypts its encryption keys. UKG does not support a "Bring Your Own Keys" option for its customers.

- Depending on the application in use by the customer, UKG maintains 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.

If an individual believes UKG maintains their personal data in one of the services within the scope of our Data Privacy Framework certification, they may direct any inquiries or complaints concerning our Data Privacy Framework compliance to privacy@ukg.com. UKG will respond within 45 days. If there is an unresolved privacy or data use concern that we have not addressed satisfactorily, they may contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request. If neither UKG nor our dispute resolution provider resolves the complaint, they may engage in binding arbitration through the Data Privacy Framework Panel. For more information, please see Annex I of the EU-U.S. Data Privacy Framework Principles.

Please visit UKG's Privacy and Data Protection page for more information.