FAQ: Data transfers in connection with UKG Dimensions, Hosted Workforce Central, and HRSD

Version: October 24, 2022

Note: while the information in this FAQ is generally applicable to UKG Dimensions and Workforce Central, it is intended to answer common questions from UKG's Europe-based customers.

	UKG Dimensions	Hosted Workforce Central	HRSD
1. Does UKG have an official statement on Schrems II?	Yes. UKG has a **Schrems II Statement** (October 24, 2022): Note that UKG products and services are subject to rigorous security requirements as is further described in the due diligence package applicable to each. UKG's products and services also comply with ISAE3402/SSAE 18 AICPA Trust Principles for Security, Confidentiality and, depending on the application, ISO 27001, 27017, and 27018.		
2. Can UKG guarantee that data is hosted / stored / processed in EU only?	No. Processing outside of the EU may occur in the following scenarios: 1. UKG **support delivery** 2. UKG **cloud security monitoring** (however, UKG database administrators generally do not have reason to access customer data) 3. **Hosted Workforce Central**: in connection with either **Workforce Central subprocessors** (and their own subprocessors where applicable). **HRSD**: in connection with **HRSD subprocessors** (and their own subprocessors where applicable). **UKG Dimensions:** in connection with **Google/cloud hosting** (e.g., Google monitoring for compliance with AUP; Google's provision of service support, which does not have geographic limitations but, in most cases, Google has to notify UKG in advance about any such access) and in connection with other **UKG Dimensions subprocessors** (and their own subprocessors where applicable) 4. However, note that the co-location service provider is **not** processing personal data 5. In connection with **UKG professional services/implementation** operations		

	UKG Dimensions	Hosted Workforce Central	HRSD
3. Can UKG confirm the locations of the data centres?	This is selected by the customer on the applicable Order Form. If the customer selects "Europe" then customer data is stored in Europe-West3 (Germany) and Europe-West 4 (Netherlands).	In Europe, Workforce Central is hosted in Equinix data centres in Germany and Netherlands.	For HRSD, the locations include (by vendor): - Rackspace (Germany) - Ecritel (France) Further information is available **here**.
4. Is any data transferred to the locations of the service support centres?	Yes. Support and/or cloud maintenance team locations for UKG Dimensions currently include the following locations: 1. United States 2. Canada 3. UK 4. Australia 5. India The above are intra-company transfers.		Support for HRSD currently includes the following locations: 1. United States 2. Singapore 3. India The above are intra-company transfers.
Has UKG made a Data Transfer Impact Assessment (DTIA) with respect to the countries to which it transfers personal data?	UKG has updated its Data Processing Agreement to include the Standard Contractual Clauses pursuant to Regulation (EU) 2016/679 and the reference to Executive Order signed on October 7, 2022. In addition, **UKG's Transfer Risk and Impact Assessment** is publicly available. Based on the information in this Statement, UKG has determined that it can proceed with the transfer of EEA/Switzerland/UK personal data. UKG's transfers of EEA/Switzerland/UK personal data are subject to the SCCs, which impose obligations intended to ensure EEA/Switzerland/UK personal data transferred to third countries is afforded a level of protection that is essentially equivalent to that guaranteed by the data protection laws of the EEA/Switzerland/UK. Furthermore, given the supplementary measures implemented, UKG has come to the conclusions that:		

	- processing primarily HR data, UKG Services & Offerings are in essence not likely to fall within the scope of bulk surveillance programs conducted by U.S. intelligence services under FISA 702 and E.O. 12333 within the meaning of the Schrems 2 ruling by the Court of Justice of the European Union; - in addition, UKG technical measures, organizational measures are in place to challenge any intelligence services access requests under FISA 702 and E.O.12333; - all of which that are likely to prevent access from unauthorized third parties including U.S. intelligence services and, as a result, to ensure effectiveness of the rights and freedoms of EEA/Swiss/UK data subjects. In addition, the US government has adopted on October 7, 2022, a new Data Privacy Framework (new Executive Order and Department of Justice Regulations), which imposes new limits on the collection and use of personal data by U.S. intelligence agencies. It also creates a new "redress" mechanism by authorizing and directing the Attorney General to establish a Data Protection Review Court (DPRC), empowered to issue decisions on alleged violations of U.S. law, that will be binding on U.S. intelligence agencies, which will be required to implement "appropriate remediation."
5. What is UKG's position in connection with rights that governmental agencies may have to require UKG to hand over data?	UKG includes the following contractual assurances: *12.1 UKG shall maintain the following additional safeguards with respect to Customer Personal Data that is transferred pursuant to the Standard Contractual Clauses:* *12.1.1 UKG agrees to notify Customer of any request from law enforcement authority or other governmental authority with competent authority and jurisdiction over UKG for disclosure of Customer Personal Data processed under this DPA ("Disclosure Request") to the extent permitted by applicable law. UKG shall not respond to Disclosure Requests without notifying Customer and receiving written authorization from Customer to respond to such Disclosure Request, except as required under applicable law or order of court or governmental authority with competent authority and jurisdiction over same;* *12.1.2 In the event UKG receives a Disclosure Request for disclosure of Customer Personal Data processed under this DPA and Data Processor is not legally permitted to notify Customer of the Disclosure Request, UKG agrees to take reasonable legal actions against the disclosure of the Customer Personal Data and to refrain from disclosure of the Customer Personal Data to the respective authorities until a court of competent jurisdiction orders UKG to disclose such Customer Personal Data. In such event, UKG agrees to provide the minimum*

	amount of information required when responding to the Disclosure Request, based on UKG's reasonable interpretation of the Disclosure Request. ***UKG's Transfer Risk and Impact Assessment*** *is available to assist Customer in carrying out its own transfer impact assessment related to Customer's use of the Services.* *For additional information, please see* ***UKG's Transparency Report – Government Requests****.*

Disclaimer:

This FAQ is for information purposes only and it does not constitute legal or other advice on how to achieve operational privacy and security. If you require legal advice on the requirements of the General Data Protection Regulation or any other law, consult a qualified legal professional. If you require advice on the technical and organisational measures that are required to deliver operational privacy and security in your organisation, consult a qualified privacy and security professional.

The information provided here is subject to change without notice and is provided without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance. If you have a question about your particular situation or circumstance, contact your UKG representative for more information.