

CROSS-BORDER DATA TRANSFER

Are there any restrictions on transferring personal data and how can these be overcome?

Cross-border data transfers affect all organizations that engage online IT services, cloud-based services, remote access services and global HR databases. Understanding the applications of lawful data transfer mechanisms is essential to validate recipients located in other nations. Data transfers typically include the following examples:

- personal data communicated over the telephone, by email, fax, letter, through a web tool or in person to another country;
- IT systems or data feeds which lead to personal data being stored on databases hosted outside the country;
- people/entities outside the country being able to access or "see" personal data held in the country; and
- the use of personal data by third parties through external solutions, e.g., outsourcing, offshoring and cloud computing.



- the ingathering and the processing of data;
- the possession, use and transfer of data;
- the reliability and up-to-datedness of the data;
- the granting of rights to view data and amend it; and,
- the obligation to take appropriate security measures to protect the data.

regulates the transfer of personal data from Israeli databases internationally. Under the TR, personal data can be transferred outside Israel when the receiving country ensures a level of data protection that is at least equivalent to the level of protection provided under Israel's laws. There are a number of principles that should be considered when determining whether a country provides an adequate level or protection, including principles which relate to:

As of July 2020, Israel's data protection authority, the Protection of Privacy Authority (PPA), has officially recognized only the European Union and the United Kingdom as having an adequate level of protection.

In cases where a country is not considered to have adequate protection, there are several conditions which, if one is met, can enable the international transfer of personal data outside of Israel. These include:



In Israel, the Protection of Privacy Regulations (Transfer of Data to Databases Outside the State's Borders), 2001 (TR):

- consent to the transfer from the employee or other data subject;
- when the transfer of the data is vital for the protection the data subject's health or physical wellbeing and consent cannot be obtained;
- when the data is being transferred to a corporation under the control of the owner of the Israeli database (i.e. the Israeli employer) and it has ensured the protection of privacy following the transfer;
- when data is being transferred to someone who has undertaken an agreement with the owner of the Israeli database to fulfill the conditions laid down in Israel for maintaining and using the data;
- when data has been published or has been opened to the public by a legal authority;
- when the transfer of the data is necessary for the protection of public welfare or security;
- when the transfer is obligatory under Israeli law; or,
- when the data is being transferred to a database in a country in which one of the following conditions exists: (1) the country is a party to the

European Convention for the Protection of the Individual with regard to Automatic Processing of Personal Information; (2) the country receives data from Member States of the European Union, under the same conditions of receipt; or, (3) the PPA has officially permitted transfers to that country under an arrangement for cooperation with the authority.



HR Best Practices: The use of applications in the cloud frequently results in the international transfer of

employee data. When transferring data outside of Israel, employers must ensure (via a written obligation from the recipient of the data), that the recipient is taking steps to ensure the privacy of the person to whom the data relates, and that the recipient has undertaken that the data is not being transferred to any person other than the recipient.

Last updated December 2021.

DISCLAIMER: The information contained in this document is for general information purposes only and is not intended to be a source for legal, tax, or any other professional advice and should not be relied upon as such. This information is not intended to create, and the receipt of it by the reader does not constitute, an attorney-client relationship. All legal or tax questions or concerns should be directed to your legal counsel or tax consultant. Laws and regulations may change and UKG Inc. ("UKG") cannot guarantee that all the information in this document is accurate, current or complete. UKG MAKES NO REPRESENTATION OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE DOCUMENT OR THE INFORMATION OR CONTENT CONTAINED HEREIN AND SPECIFICALLY DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES INCLUDING BUT NOT LIMITED TO ANY EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY, OR COMPLETENESS OF THIS INFORMATION. TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, NEITHER UKG, NOR ITS AGENTS, OFFICERS, EMPLOYEES, SUBSIDIARIES, OR AFFILIATES, ARE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF USE OR PROFITS, OR BUSINESS INTERRUPTION), EVEN IF THE UKG HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT, ARISING IN ANY WAY OUT OF THE USE OF OR INABILITY TO USE THIS INFORMATION. This document and the content are proprietary and confidential information of UKG. No part of this document or its content may be reproduced in any form, or by any means, or distributed to any third party without the prior written consent of UKG © 2021 UKG Inc. All rights reserved.