



# Employee Data Privacy – Israel

## Breach Notification

### Are there any data breach notification requirements?

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Local data protection regulations have required data controllers to report such breaches in certain circumstances.



Israel's Protection of Privacy Regulations (Data Security), 2017 (DSRs) includes the requirement that in the event of a

Severe Security Incident, owners of databases must immediately notify the Registrar. Whether an incident is considered "Severe" depends in part on the level of security required for the database (basic, medium or high) under the DSR.

HR databases are generally classified as subject to the basic level of security unless the database includes data relating to 100,000 or more individuals or, if there are 100 or more individuals who have access to the database. In these cases, the database is subject to a high level of security.

In a database that is subject to a high security level, an event where data from the database was used without or in breach of an authorization or, where harm was caused to the integrity of the

data is considered a Severe Security Incident. For a database subject to a medium security level, an event where a material part of the database was used without or in breach of an authorization or, where harm was caused to the integrity of the data in respect of a material part of the database is considered a Severe Security Incident.

If an employer experiences a Severe Security Incident, the Registrar should be notified immediately, generally within 24 hours (and no later than 72 hours) of becoming aware of the incident. The notification to the Registrar should include a report of steps that are being taken as a result of the event.

The Registrar may, after consulting with the head of the National Authority for Cyber Security, order the employer or other owner of the database to notify affected data subjects who are likely to be harmed by the data breach.



### HR Best Practices:

Employers should develop and implement a data breach action plan with notification, incident documentation and response procedures. In cases where notification is not required by law, employers should consider whether notification should be given to the Registrar and/or impacted individuals in order to mitigate potential damages.

Last updated November 2022.

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 © 2022 UKG Inc. All rights reserved.