

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.



The General Data Protection Regulation (GDPR) requires data controllers to notify data protection authorities (DPAs) of a data breach when such breach is “likely to result in harm for data subjects.” For example, a breach that unveils employee salaries or bank-related information can be considered likely to result in harm, since this information can be used for further hacking.

Last updated December 2020.

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 © 2020 UKG Inc. All rights reserved.

The breach must be reported to the DPA within 72 hours of becoming aware of a potential breach and without undue delay. If there is a delay, the Controller should include the reasons for not being able to notify the DPA within the 72-hour timeframe.

Regarding notification to the data subjects affected, the GDPR exempts the data subjects' notification if the risk of harm is remote because the data affected was protected (through encryption, for example) or the notification requires disproportionate effort (in this case a public notice must be issued).

HR Best Practices: Employers should develop and implement a data breach action plan with notification, incident documentation and response procedures. Written agreements with sub-processors should clearly outline responsibilities in the event of a data breach and include that sub-processors must notify data controllers of a breach without undue delay. Incidents in the employment context which might trigger a requirement to notify include a laptop or file left on a train, or an email containing HR information sent massively to incorrect addresses. However, a breach does not have to be notified to the DPA if it is unlikely to result in risk for the rights and freedoms of individuals (e.g. the personal data on the lost laptop is protected by encryption).