

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.

General Data Privacy Law Security Incident Requirements

Under Brazil's General Data Privacy Law, employers (and other data controllers) are required to inform the data protection authority (ANPD) and the data subject if a security incident which may create risk or damages to the data subjects occurs.

The communication should include:

- a description of the nature of affected personal information;
- information on the data subjects involved;
- an explanation of the technical and security measures that were used to protect the data (subject to commercial and industry secrecy);
- the potential risks related to the incident;
- measures that are being taken to reverse or mitigate the damages that may occur as a result of the breach; and,
- if there is a delay in communicating the incident, the reasons for the delay.

Last updated November 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.

The ANPD has a security incident reporting form which includes additional requested information.



Individual unauthorized information disclosures or access may be resolved directly between the employer (as the data controller) and the employee (as the impacted data subject). In the event that there is no agreement, the employer would be subject to the penalties.

The ANPD has issued preliminary guidance relating to security incidents and is working on a formal Resolution. In the interim, the ANPD recommends reporting the incident as soon as possible and within two business days from identifying the incident. More detailed instructions relating to responding to a data breach may be announced by the national data protection authority in the future.