

## SECURITY REQUIREMENTS

### What security obligations are imposed on data controllers and data processors?

Security requirements may not always be included in the data protection law, but are key to guaranteeing lawful processing of personal data. The entity processing the data must take all useful precautions with respect to the nature of the data and the risk presented by the processing, to preserve the security of the data and, prevent alteration, corruption or access by unauthorized third parties. Appropriate technical and organizational measures should be implemented to ensure a level of security appropriate to the risk.



The General Data Privacy Law (LGPD) requires that those who process personal data adopt security, technical and administrative measures to protect personal information from unauthorized access, accidental or unlawful destruction/loss/alteration/communication or other unlawful processing. More detailed rules may be issued by the data protection authority in the future.

When handling personal employee data, recruiting data, and communications, employers should consider the following as a best practice:

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.

- Limit who can access personal data and private communications and, develop mechanisms to authenticate individuals (and prevent unauthorized access).
- Protect data through IT security programs and mechanisms, such as encryption.
- Use detailed access logs which track the records accessed, the time and duration of access and the identity of the individual who viewed/modified data.
- Train employees on data processing procedures, security measures and data breach procedures.
- Implement data processing agreements with vendors and service providers.
- Ensure incident response and remediation plans are in place.
- Establish policies and safeguards based on systematic assessments of potential privacy risks and impacts.



### HR Best Practices:

Regularly review personal information that you maintain for your employees and take all reasonable measures to protect personal information, such as limiting access to data and training employees on security measures.