



# Employee Data Privacy – India

## 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.

Companies should take reasonable security measures to protect Sensitive Personal Data or



Information (SPDI), per India's Information Technology Rules, 2011 on Reasonable Security

Practices and Procedures and Sensitive Personal Data or Information ("Privacy Rules"). These measures are expected to include a comprehensive, documented information security program and policies which contain managerial, technical, operational and physical security

control measures. In addition, the measures taken should reflect the sensitivity of the information and the nature of the business.

Whatever security standards are followed, they should be certified or audited at least once a year by an independent auditor. India's Privacy Rules include reference to the IS/ISO/IEC 27001 "Information Technology - Security Techniques - Information Security Management System - Requirements" as an appropriate standard.

That said, note that if parties agree on what constitutes reasonable security practices/procedures, the parties can agree to exclude the applicability of the Privacy Rules.



### HR Best Practices:

Review personal information that you maintain for your employees and take all

reasonable measures to protect sensitive personal information, including regularly training employees on security measures and controls. Ensure all processes and controls are clearly documented and regularly tested to ensure procedures are being followed.

Last updated July 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.