



Employee Data Privacy – Chile

Employee Consent

Do I have to obtain employees' consent in order to collect their personal data?

The processing of any personal data may impose obligations to the individuals the data is related to, the data subjects. Some jurisdictions only recognize processing personal data as lawful if the data subject has provided express consent. Other jurisdictions require a legal obligation to process the data and may not require consent. The processing of HR personal data has raised questions and court decisions in a few countries, and interpretations may vary based on data privacy and labor law requirements. The concept of employee consent has been increasingly criticized because there is doubt as to whether consent can be given freely in the subordinate employee/employer relationship.

In Chile, employers can only process employee data with the employee's express and explicit consent, except when the processing of personal information is otherwise permitted by law or when the personal data is collected from publicly accessible sources (Personal Data Protection Law, 19628). Likewise, no authorization is required for the processing of personal data made by private legal entities for their exclusive use, its associates and entities that are affiliated with statistical purposes, pricing or other general benefits. Employees (and other individuals) must be informed about the purpose of the storage and must give their consent in writing. Individuals can later revoke consent to having their personal data

processed in writing, but this only applies on a go-forward basis.



When employers provide information in order to obtain the data subject's written consent, the document should inform the individual of: the purpose of the collection and storage of their personally identifiable information; and, the possible communication to the public (e.g. the purpose of fulfilling the employer's labor obligations, improving and maintaining the administration of the company, facilitating expense tracking and budgeting, tracking assignments, improving and maintaining security systems, etc.). This information can be included in the employment contract or in an addendum to the employment contract and should be provided before processing the data.

UKG HR COMPLIANCE ASSIST

Sensitive Personal Data



There are additional restrictions when processing sensitive data. Sensitive

personal data includes physical or moral characteristics, such as personal habits, racial origin, ideologies and political opinions, beliefs/religious convictions, physical/mental health and sexual life. In principle, sensitive personal data cannot be processed by employers. All personal information (sensitive or not; including medical files) should be managed with due confidentiality. Only as an exception, and with the employee's consent, can certain

sensitive data be processed when strictly necessary for the determination or granting of health benefits, or when specifically authorized by law (e.g. the IRS in relation to the information of the taxpayers and the Ministry of Health in relation to contagious diseases).



HR Best Practices:

Build consent for data collection into employee contracts/addendums

and onboarding agreements. Ensure individuals are clearly informed about the reasons that their data will be processed. If the purpose of the processing changes, employers will need to have employees consent to the new purpose in writing.

Last updated February 2023.

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 © 2023 UKG Inc. All rights reserved.