

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.

China's Cybersecurity Law requires that network operators obtain consent from data subjects in order to collect and use their personal information. "Network operators" primarily applies to organizations who collect information from website users. That said, no guidance or regulation currently defines whether "network operators" includes employers who are processing their employees' personal information.

Some employers follow The Personal Information Security Specification, (个人信息安全规范, GB/T 35273-2020) when collecting employee data. The Specification includes suggested best practices for personal data controllers (business and individuals who process personal data), such as:

- obtaining the employee's consent to the collection/use/disclosure of their personal data;
- providing employees with a notification which includes: the purposes, means, scope and rules for the collection and use of personal information.



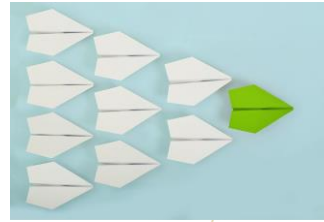
The Specification includes additional restrictions when processing sensitive personal information (ex. bank account numbers, personal health information, biometric data, personal identification numbers, network identification information, personal phone numbers, marriage history, religious beliefs, sexual orientation, undisclosed criminal records, geographical location, internet browsing history, etc.) According to the 2020 Specification, HR data may be considered sensitive personal information because it often contains personal identification information and some health information. When processing sensitive personal information and personal biometric information, employers should

obtain express consent from employees and job applicants. Express consent should be specific, clear, unambiguous and voluntarily given.

Under the Specification, businesses do not have to obtain consent in certain cases, such as when:

- directly related to fulfilling the legal obligations of the data controller (such as the employer);
- directly related to national security;
- related to a trial, criminal investigation, prosecution or execution of judgments;
- protecting life, property, or material legal rights of individuals; or,

- directly related to public safety/public health/public interests.



HR Best Practices:

Make sure to have an up-to-date privacy policy, which includes a clear and reasonable purpose for collecting employees' personal information. Follow the best practices outlined in the Specification to obtain employee consent to process personal employee data.

Last updated May 2020.

DISCLAIMER: The information contained in this form is for general information purposes only and is not intended to be a source for legal, or any other 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. Organizations or individuals receiving this document should always seek the advice of competent counsel in their home jurisdiction. Laws may change and The Ultimate Software Group, Inc. cannot guarantee that all the information in this form is current or correct. THE ULTIMATE SOFTWARE GROUP, INC. MAKES NO REPRESENTATION OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE DOCUMENT OR CONTENT 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 THE ULTIMATE SOFTWARE GROUP, INC., 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 ULTIMATE SOFTWARE GROUP, INC 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 The Ultimate Software Group, Inc. No part of this document or content may be reproduced in any form or distributed to any third party without the written consent of The Ultimate Software Group, Inc. © 2020 The Ultimate Software Group, Inc. All rights reserved.

PeopleDoc HR Compliance Assist

HR Compliance Assist helps companies manage compliance of their HR files and employees' data with foreign laws and regulations. The HR Compliance Assist team works with an international network of lawyers to provide best practices on topics such as HR document retention, employee data privacy, electronic signature and electronic archiving.

HR Compliance Assist is available to customers of PeopleDoc by Ultimate Software, a leading HR Service Delivery provider. In 2018, PeopleDoc joined Ultimate Software, a leading provider of human capital management cloud solutions. Today, Ultimate serves approximately 4,500 customers with employees in 180 countries.

More information about PeopleDoc by Ultimate Software can be found at www.people-doc.com.



HR Compliance Assist

www.hrcomplianceassist.com - hrcomplianceassist@people-doc.com