

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. Employers in Finland should follow the general security standards listed in Article 32 of the General Data Protection Regulation. When protecting employee and applicant data, consider

the sensitivity of the information, the technology available, the expense of protecting the data and the risk to individuals if the data is compromised. Then take organizational and technological measures, including:

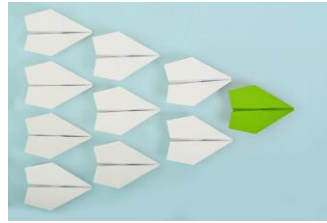
- pseudonymization/encryption;
- measures to ensure the confidentiality, integrity, availability and resilience of information processing systems
- measures to restore the system and access in case of an incident (such as a power outage)
- processes to regularly test and assess the system to ensure continued security.

The Finnish Data Protection Act (1050/2018) (DPA) also includes certain security requirements relating to employee data processing, including:

- giving those who process personal data a duty of confidentiality; and,
- prohibiting personal identity numbers from being unnecessarily included on printed hard copies or drawn up from personal data files.

Separately, processing employees' medical data is limited under the Finnish Act on the Protection of Privacy in Working Life (759/2004). Employers may

only process medical data for purposes specified in the Act or when allowed by other laws. In addition, only certain individuals can process employees' health information (those in specific roles or those who have been nominated). The employer and those who are permitted to process health-related data are subject to non-disclosure obligations and cannot disclose employees' health information to third parties. Any information relating to an employee's state of health should be stored separately from other personal employee information.



HR Best Practices: Ensure contracts with service providers detail the security and confidentiality measures

that will be implemented. In addition, regularly train employees who may have access to personal information, to ensure that they are following all technical and organizational security measures that have been put in place.

Last updated June 2019.

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. © 2019 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