

## EMPLOYEE ACCESS RIGHTS

### Do individuals have the right to access their personal information?

Data protective jurisdictions tend to guarantee the right of individuals to contact an organization directly and find out whether personal data is being tracked. Access procedures and acceptable exceptions (such as business secrecy) are determined by law and may be subject to the control of data protection authorities. In the context of HR, personal data access requests can include information tracked by the company as well as data tracked by third-party solutions, such as background check vendors.

Data subjects have the right to request and obtain confirmation as to whether their personal data is being processed. Where that is the case, individuals must be able to access their personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients or categories of recipients to whom the personal data has been or will be disclosed, in particular recipients in third countries or international organizations;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the existence of the right to: request rectification or erasure of personal data; request restriction of processing data concerning the data subject; or, to object to such processing;
- the right to lodge a complaint with a supervisory authority.

Every person may directly request that the data be corrected, completed, clarified or erased. Requests can be sent directly to the data controller or to any other actor in the chain of processing. The processors and sub-processors have the obligation to inform the

data controller of any request regarding a data subject and shall only proceed with the request under data controller's instructions. Therefore, the processor shall, whenever possible, assist the data controller with data subjects' requests.

As a general rule, the access request shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, a reasonable fee may be charged. Fees should take into account the administrative cost of providing the information or taking the action requested.



Requests must be answered within one month of receipt of the request. Any delay should be justified and accompany the

request response. The format of the response should be based on the means used to make the request, unless otherwise requested by the data subject. In other words, if a request is emailed, the response should be via email unless the individual requests a mailed letter.

Where the controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject. However, a reasonable proof of identity is always recommended.

Every person may contact the relevant data protection authority within the European Economic Area to receive assistance in the exercise of his or her rights (particularly if the right of access has been denied).

## Compensation

If a data controller causes harm to a data subject by collecting, processing or using an individual's personal data in violation of data protection regulations, the controller must compensate the data subject for the harm caused. There are no punitive damages under German law. The right to claim compensation also applies if the personal data is stored by non-automated procedures or filing systems. This obligation will not apply if the data controller has exercised due care in accordance with the circumstances of the specific case.

## German Federal Data Protection Law

A few data subject rights were restricted in Germany's Federal Data Protection Act, including:

- **Right of access:** If an employee's personal data is only stored to comply with statutory retention provisions, or for the purposes of data backup or monitoring, the access right doesn't apply. The

right also doesn't apply in cases where giving access to the employee or individual would reveal confidential data (including private information on third parties or trade secrets). When access requests are refused, the reasons behind the refusal should be documented.

- **Right to erasure:** The controller (i.e., the employer) is exempt from the obligation to erase personal data when erasure is, in case of non-automatic data processing, impossible, or only possible with disproportionately high effort and the data subject has a minor interest for erasure.



### HR Best Practices:

When processing an access request from an employee, make sure not to disclose information connected to other employees. Processors and sub-processors should establish official procedures and contacts for employee requests.

Last updated March 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](http://www.people-doc.com).



HR Compliance Assist

[www.hrcomplianceassist.com](http://www.hrcomplianceassist.com) - [hrcomplianceassist@people-doc.com](mailto:hrcomplianceassist@people-doc.com)