

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.

Employees and job applicants are generally allowed access to their personal data under the Personal Data Protection Act 2012 (PDPA, Sec. 21). In addition, employers must generally notify employees prior to data collection/use/disclosure (excluding for evaluative purposes).



Employee Access

Upon request, employers should provide individuals with the personal data about the individual that is under the control of the employer. In addition, employers should provide information as to the ways the personal data has been or may have been used

or disclosed in the year prior to the request. Some data is exempt from this requirement, such as:

- personal data that would reveal personal data about another individual;
- personal data that would threaten the safety, physical or mental health of an individual;
- opinion data kept solely for an evaluative purpose (such as job candidate reviews);
- personal data subject to legal privilege;
- personal data, which, if disclosed, could in the opinion of a reasonable person, harm the competitive position of the organization;
- requests that would: unreasonably interfere with the operations of the organization due to the systemic nature of the requests; be unreasonable or disproportionate to the individual's interests; not be possible as the data doesn't exist/can't be found; or is otherwise frivolous or vexatious.

Organizations can charge a reasonable fee to process access requests in order to cover the incremental costs associated with responding to a request.

Access should be provided to employees as soon as reasonably possible. If it will take more than 30 days to respond to an access request, inform the employee within 30 days as to when the response will be provided (employers should provide access at the soonest possible time).

Correction/Withdrawal Requests

Employers should correct personal data upon an individual's request unless there are reasonable grounds that the correction should not be made. If a correction is made, the employer should send the updated data to every other organization to which

the personal data was disclosed in the last year before the date the correction was made.

Employers do not need to correct personal data where:

- the personal data was only kept for an evaluative purpose;
- the data is relating to a legal claim that hasn't been completed.

Note that organizations **cannot** charge a fee to process a correction request.

If it will take more than 30 days to respond to a correction request, inform the employee in writing within 30 days as to when the correction can be made (information should be corrected at the earliest feasible time).

Personal Data Protection (Amendment) Act 2020

The Ministry of Communications and the Personal Data Protection Commission (PDPC) have passed amendments to the existing Personal Data Protection Act 2012. These amendments will take effect in phases, starting in February 2021. The enhanced PDPA includes additional access requirements, including that:

- organizations would be required to retain personal data requested pursuant in an access request (or a copy) for at least 30 calendar days after rejection of the request or, until the individual has exhausted their right to apply for reconsideration to the PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal (whichever is later);
- organizations may have a data portability obligation for data held electronically (i.e., organizations may, at the request of an individual, be required to transmit personal data that is in the organization's possession or under its control, to another organization in a commonly used machine-readable format).

If the amendments are passed these requirements may impact employers in the future.



HR Best Practices:

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

Last updated February 2021.

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 © 2021 UKG Inc. All rights reserved.