

BREACH NOTIFICATION

Are there any data breach notification requirements?

A data breach is a security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so. Local data protection regulations have required data controllers to report such breaches in certain circumstances.



The Ministry of Communications and the Personal Data Protection Commission (PDPC) have passed amendments to the existing Personal Data Protection Act 2012 (PDPA), which went into effect, in part, on February 1, 2021. The enhanced PDPA includes a mandatory breach notification in the event of a data breach that is likely to result in significant harm or impact to individuals or, if the breach is of a significant scale (i.e. There are 500 or more impacted individuals).

In addition, employers and other organizations are required to notify the PDPC as soon as practicable and no later than three days after determining whether the breach meets the required notification threshold. Employers and other organizations are also, with few exceptions, required to notify individuals if a breach is likely to result in significant harm or impact to affected individuals.

When notifying the PDPC, include the following information (Personal Data Protection (Notification of Data Breaches) Regulations 2021, Art. 5):

- the date and circumstance which the employer first became aware of the data breach;
- chronological account of the steps taken after becoming aware that a data breach occurred;
- how the notifiable breach occurred;
- the number of affected individuals;
- the personal data or classes of personal data affected;
- potential harm to affected individuals;
- information on actions taken by the employer or actions that will be taken by the employer to eliminate/mitigate potential harm to affected individuals and, to address/remedy any failures/shortcomings that the employer

believes caused, enabled or facilitated the breach;

- information on the plan (if any) to inform affected individuals or the public that the data breach occurred and how affected individuals may eliminate/mitigate potential harm;
- business contact information of the employer's authorized representative(s).

Employers should consider alerting the police in the event criminal activity is suspected. In the event of a suspected cyberattack, employers may also alert the Cyber Security Agency of Singapore through the Singapore Computer Emergency Response Team (SingCERT).



HR Best Practices: Having a data breach management program in place can help to ensure employers are

prepared in the event that personal employee data is compromised. The PDPC's Guide to Managing Data Breaches 2.0 (22 May 2019) recommends that programs include:

- a clear explanation of what constitutes a personal data breach;
- how a personal data breach should be reported internally (For example, knowing the individual or team who should be informed of a potential breach);
- how to respond to a breach; and,
- the responsibilities of the data breach management team (creating a clear chain of command and, determining who would be responsible for assessing risks and making critical decisions.

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.