

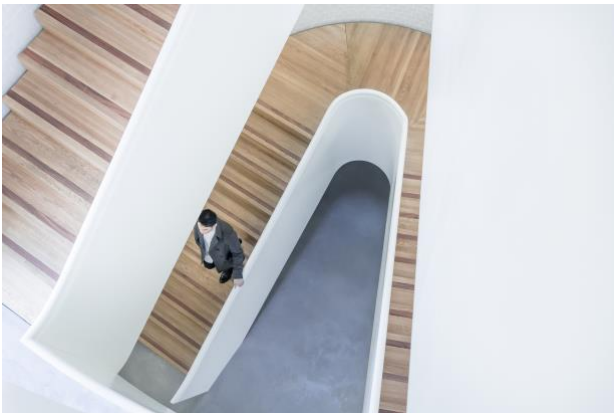


Employee Data Privacy – The Republic of the Philippines

Data Protection Officer

What is, and which organizations have to appoint a DPO?

A Data Protection Officer (DPO) is a person in charge of verifying the compliance of personal data processing with the applicable law. The DPO communicates information on processing personal data such as its: purposes, interconnections, types, categories of data subjects, length of retention and department(s) in charge of implementing processing. DPOs may be required by law or recommended.



Employers (and other information controllers and processors) must designate a DPO who is accountable for compliance with the Data Privacy Act and associated rules and regulations relating to privacy and data protection. The DPO's responsibilities include:

- monitoring compliance with the DPA and its implementing rules and related regulations;
- ensuring the conduct of Privacy Impact Assessments;
- advising the employer regarding complaints and/or the exercise by data subjects of their rights;
- ensuring proper data breach and security incident management;
- cultivating awareness on privacy and data protection;
- advocating for the development, review, and revision of data privacy guidelines; and,
- serving as the employer's contact person.

Note that with the National Privacy Commission's approval, a group of related companies can appoint/designate a DPO to be primarily accountable for ensuring data protection compliance across the entire group. In this case, each company would still need to have a Compliance Officer for Privacy (COP).

A DPO or COP's contact details must be accessible to concerned parties and must be published on the company's website and included in privacy notices, privacy policies and privacy guides. The contact details should include the title/designation, postal address, dedicated phone number, and dedicated email address. The individual's name does not need to be published but should be available if requested (NPC Advisory No. 2017-01 – Designation of Data Protection Officers).

Last updated October 2022.

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 © 2022 UKG Inc. All rights reserved.