

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. In Australia, the data security obligations in the Privacy Principles (APP 11) apply to any entity that holds Personally Identifiable Information (PII). Employers should take reasonable steps to protect PII from: misuse; interference and loss; and from unauthorized access, modification or disclosure. Reasonable steps should be determined by the entity based on:

- the sensitivity of the information;
- the volume of the data; and,
- whether the entity is similar to a data controller or a vendor/subcontractor

The Taxation Administration Act 1953 and the Income Tax Assessment Act 1936 govern the collection,

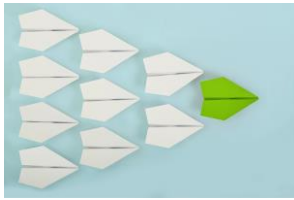
storage, use, disclosure, security and disposal of an employee's tax file numbers. Employers and any third party 'approved recipient' must take reasonable steps to protect employee tax file number (TFN) information from misuse and loss, and from unauthorized access, use, modification or disclosure.



Employers and approved recipients must also ensure that access to records containing TFN

information is restricted to individuals who need to handle that information for taxation, personal assistance or superannuation law purposes. Employers and approved recipients must also ensure all staff are aware of the need to protect privacy when handling TFNs, and that staff who collect TFN are aware of:

- the circumstances when TFN information may be collected;
- the prohibitions on the use and disclosure of TFN information;
- the need to protect privacy (including under the TFN Rule and the Privacy Act); and,
- the penalties or other sanctions for breaches of TFN privacy laws.



HR Best Practices:

Take all appropriate security measures based on the sensitivity and

confidentiality of the data. Educate employees and

other individuals who have access to data on security standards, especially those who have access to TFN information. Take reasonable steps to ensure they comply with security procedures.

Last updated June 2020.

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. © 2020 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