



Employee Data Privacy – Greece

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. Employers in Greece should follow the general security standards listed in Article 32 of the

General Data Protection Regulation. When protecting employee and applicant data, consider the sensitivity of the information, the technology available, the expense of protecting the data and the risk to individuals if the data is compromised. Then take organizational and technological measures, including:

- pseudonymization/encryption;
- measures to ensure the confidentiality, integrity, availability and resilience of information processing systems
- measures to restore the system and access in case of an incident (such as a power outage)
- processes to regularly test and assess the system to ensure continued security.

COVID Safety Guidelines

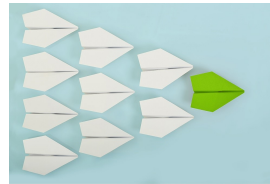
In April 2020, the Hellenic Data Protection Authority (HDPa) issued no. 2/2020 guidelines to address data safety measures in the context of remote work due to COVID. The measures include considerations for the use of email, messaging applications, terminal devices and storage while working from home. They also address network access and teleconferences.

UKG HR COMPLIANCE ASSIST

These guidelines are supplemented by Decision no. 32/2021 and the Guidelines no. 1/2021, issued on 04/08/2021 on the protection of personal data in the context of teleworking. The guidelines include the employee's right to disconnect outside of work hours, safety measures relating to bring your own device (B.Y.O.D.) policies, prohibiting the requirement of web cameras, the transfer of data to third countries and the distinction between the employee's personal and professional life.

Employers are obligated to protect home teleworkers' professional and personal data as well as inform them of actions and procedures necessary for this purpose, pursuant to Labor Law 4808/2021. Per the HDP, if personal data is

transferred to third countries during work from home, the data controller can either use tools and platforms that comply with GDPR provisions regarding data transfers to third countries or use the standard contractual clauses approved by the Europe Commission, per the HDP.



HR Best Practices:

Ensure contracts with service providers detail

the security and confidentiality measures that will be implemented. In addition, regularly train employees who may have access to personal information, to ensure that they are following all technical and organizational security measures that have been put in place.

Last updated May 2023.

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.