



Employee Data Privacy – United Kingdom

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 the United Kingdom should follow the general security standards listed in the UK Data Protection Act 2018 (UK GDPR). The Act

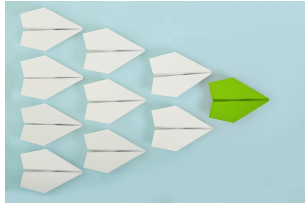
largely mirrors the European Union General Data Protection Regulation requirements. When protecting employee and applicant data, consider the sensitivity of the information, the technology available, the expense of protecting the data and the risk to individuals if the data is compromised. Then take 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.

The UK's Information Commissioner's Office (ICO) recommends that organizations should adopt best practice methodologies such as ISO 27001. In addition, the UK GDPR requires that employers put 'appropriate policy documents' in place, in certain cases, if they are processing special/sensitive information (e.g. performing criminal background checks) and, have an 'appropriate policy document' in place outlining and explaining the procedures for securing compliance with the principles of the UK GDPR.

UKG HR COMPLIANCE ASSIST

Employees should be provided with a document outlining company data retention policies.



HR Best Practices:

Ensure contracts with service providers detail the security and confidentiality measures to be implemented.

Areas that should be considered include:

- data access protection (with a clear access and password policy)
- electronic data storage
- data transfer (encryption)
- data disposal (for example, the data processor can commit to take all necessary steps to ensure that all business-critical information is removed from any decommissioned computers or external drives)
- employee awareness (through training programs and similar)

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.