

Employee Data Privacy – Belgium

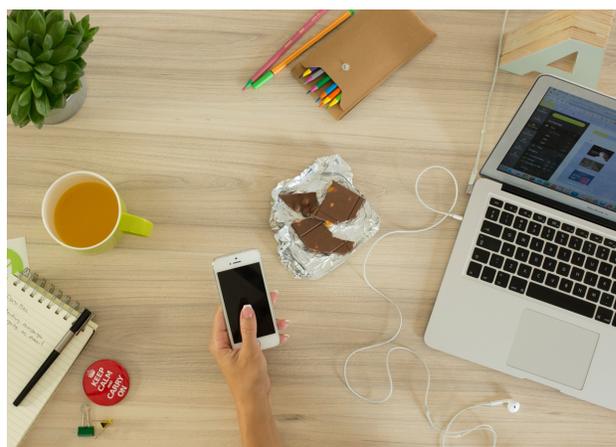
Registration Requirements

Does HR data processing require registration under data protection laws?

Data protection laws sometimes include conformity assessments, which help to ensure businesses follow regulations. Requirements can include registration before the Data Protection Authority and random audits. The General Data Protection Regulation (GDPR), which became effective on May 25, 2018, has helped make the requirements within the European Economic Area more uniform. That said, each Data Protection Authority remains independent and can create their own conformity assessments.

The GDPR is oriented on “privacy by design” and “privacy by default.” Controllers (employers) and Processors (subcontractors) must implement all technical and organizational measures necessary to ensure the protection of personal data. In practical terms, the processing of personal data in every instance should be accompanied with the privacy concern in order to limit the amount of data processed from the outset (so-called "minimization" principle). HR teams should think carefully before collecting any new piece of data. Two key considerations are the reasons for collecting the data and the potential consequences (risks) of maintaining and processing this data.

The consequence of this accountability principle is the reduction of required employee notifications once controllers and processors conclude that processing the personal data does not constitute a risk to privacy. Prior to the GDPR going into effect, processing personal data was subject to authorization from the competent data protection authority. Going forward, the new procedure will involve privacy impact assessments.



The GDPR has a few new compliance requirements to demonstrate accountability, such as:

- maintaining a register of treatments implemented
- the notification of security breaches (to the authorities and persons concerned)
- certifications
- adherence to codes of conduct

UKG HR COMPLIANCE ASSIST

- the DPO (Data Protection Officer)
- Privacy Impact Assessments (PIAs)

Works Council Requirements

While employers in Belgium are not required to register with the data protection authorities, there are cases where the works council and/or employees will need to be informed prior to implementing technology that may impact employee privacy. This includes:

- Collective Bargaining Agreement 68 of June 6 1998, which places requirements on employers including the requirement to notify the local works council prior to posting cameras in the workplace;
- the updated Camera Surveillance Act (March 2018), which requires employees to be informed when video surveillance is used by the employer (this can be done via a privacy policy). The Act also contains the obligation to keep a register of camera surveillance related activities (including publicly disclosed visuals of where the cameras are placed) until video surveillance ends. Note that recordings generally must be destroyed within one month;

- Collective Bargaining Agreement 81 of 26 April 2002 on the protection of workers' privacy with regard to the control of networked electronic communication data. This Agreement requires employers to inform the works council prior to installing an electronic communication data control system. Monitoring the use of employee email and internet access is limited to what's proportionally appropriate given the reason for monitoring. Permitted reasons are limited (ex. securing systems, preventing illicit/defamatory facts, protecting the financial interests of the company, etc.).



HR Best Practices:

When appropriate, consider looping in the works council when new data

collection practices are being put in place. Build in privacy considerations and risk assessments for all employee and candidate data collection processes. Follow the principles of “privacy by design” and “privacy by default.”

Last updated March 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.