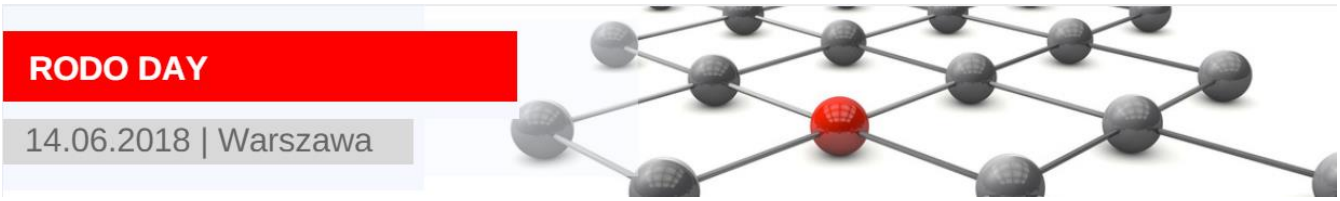


Dear Readers,

The provisions of the GDPR are being applied starting from 25 May. Moreover, the Personal Data Protection Act was passed on 16 May. It introduced in particular important changes into the Labor Code with respect to the surveillance of employees at the workplace, including the use of visual and email surveillance.

At the same time, work is ongoing on changes to laws on the personal data that can be processed by the employer during recruitment and during employment.

In this issue of PRO HR, we are commenting on the key changes and suggesting how to prepare for the new legal reality, especially given the lack of transitional regulations and a clear interpretation of the GDPR.

We hope that you will find the May issue of ProHR useful, along with the GDPR Decalogue we have prepared especially for you.

Wishing you a rewarding read,
Dominika Dorre-Kolasa

What 25 May 2018 means for the day-to-day functioning of data processing entities – the implementation and application of the GDPR

The GDPR came into force already back in 2016, but only starting on 25 May it is applicable in full, regardless of the advancement of the legislative work on changes to industry-level regulations. This entails new duties for employers and means that they have to verify the documentation they are currently using.

EVENTS

GDPR Day
14 June 2018

GDPR Day is dedicated to managers, HR employees and representatives of personal data processors.

A paid event.

The program is available here.

The conference will be held on **14 June 2018 (Thursday) at 09:30 – 16:30**, at our offices at 17 Bonifraterska (floor 21) in Warsaw.

Please send your questions and applications to prohrevents@raczkowski.eu

GDPR DECALOGUE

1. Do not give in to the GDPR panic. Keep calm and pursue your implementation plan consistently and professionally.

2. Evaluate the risk and monitor its level. For all personal data processing, the level of personal data processing risk should be determined and appropriate preventive measures should be implemented.

3. Be precise about cataloguing and cleaning up personal data. This is the only way to assess the risk of personal data breach (e.g. you should check what data are processed, how many people have access to them and for what purposes, what the archives look like, what registers are being maintained and by whom, what your employees collect in their cabinets etc.).

4. Be careful when issuing authorizations and entrusting personal data processing. In order to implement the GDPR correctly, you must identify operations of data processing where processing is entrusted to another party. Do not sign contracts with suppliers whom you have not assessed with respect to whether they can guarantee that adequate technical and organizational measures will be implemented. **Remember!** Every person authorized by the data controller or the data processor who has access to personal data processes them solely at the controller's request!

5. Determine to whom and at what time the required information will be sent. Review your current data processing clauses for the requirements stemming from Art. 13 and 14 of the GDPR so that starting on May 25 these requirements are met for processing that begins after that date.

6. Process only what is necessary. Remember that the data you are processing must be adequate, relevant and limited to what is necessary for the purposes for which they are processed.

7. Design solutions that are adequate for your organization. Remember that the GDPR requires an individualized approach to personal data processing at your organization, and this requires a considerable time investment. Cutting corners by using ready-made templates could lead you astray.

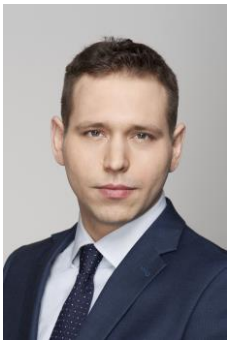
8. Develop the required documentation. It is the duty of controllers and processors to prepare appropriate documentation. The contents of the documents should depend on the risk assessment for different data processing operations.

9. Do not collect any extra data (for later) and don't store the data you don't need anymore. Remember that personal data should be collected for specific, explicit and legitimate purposes and should not be processed further in a way that is incompatible with these purposes, and that they should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

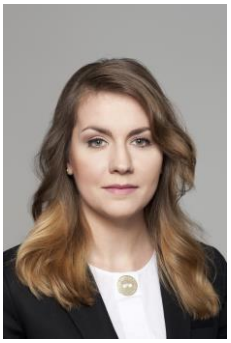
10. Remember that consent is not a cure for all illnesses. Ask for consent only when there is no other legal basis for processing. Remember that if the data minimization principle is violated, i.e. the principle that data should be limited to what is necessary for the purposes for which they are processed, a consent will not legitimize this violation.

Ius Laboris Poland Global HR Lawyers
Raczkowski Paruch

When processing personal data, you will have to design and implement a comprehensive system for the protection of such, which will be adjusted to the nature of your business and your organization, as well as to ensure the accountability of your actions (the ability to demonstrate your actions in this area). In order to do this, I recommend a thorough verification of your personal data as well as determining the purpose and the period of their processing. Failure to comply with GDPR requirements might result in an inspection, and if irregularities are found, severe penalties could be imposed.



trainee advocate
Jakub Lasek



If you entrust the processing of the personal data of your employees to other parties (e.g. when human resources and payroll services are outsourced), I recommend taking a closer look at the current data processing agreements. GDPR significantly expands the regulations pertaining to such agreements.

trainee advocate
Paulina Szymczak-Kamińska

In particular, as a controller you can only entrust personal data processing to entities that provide a sufficient guarantee that they will implement appropriate technical and organizational measures for the processing to meet the requirements laid down in the GDPR, with protection of the rights of the data subjects. As far the content of the data processing agreement is concerned, you should remember that the mandatory elements of data processing agreements include, inter alia, (1) the subject and the term of the processing, (2) the nature of the purpose of the processing, (3) the type of the personal data and the categories of the data subjects and (4) the duties and rights of the controller. It is a good idea to review your agreements for the inclusion of all the required information and to verify whether the processor to whom you entrust the data gives them adequate protection.

Should every employer appoint a personal data protection officer?

The GDPR does not require that all employers appoint a data protection officer. The appointment must be made if the processing is done by public authorities, as well as entities for which (1) the core activities consist of large-scale data processing operations, and the nature, scope and purposes of this processing require regular and systematic monitoring of data subjects, or (2) the core activities consist of processing on a large scale of special categories of data (as specified in Article 9 of the GDPR) or data relating to criminal convictions. Determining whether this requirement arises is one of the employer's internal tasks, and this assessment should be justified (i.e. documented).

trainee legal advisor
Grzegorz Larek

Appointing a competent data protection officer voluntarily may be helpful, because their support will facilitate compliance with the rules and help prepare the required documentation, and they will be in charge of the day-to-day contact with supervisory authorities. On the other hand, it is hard to imagine that one person should be able to fulfill all the duties stemming from the GDPR. It should be remembered that, as a rule, the personal data protection officer should be a natural person.

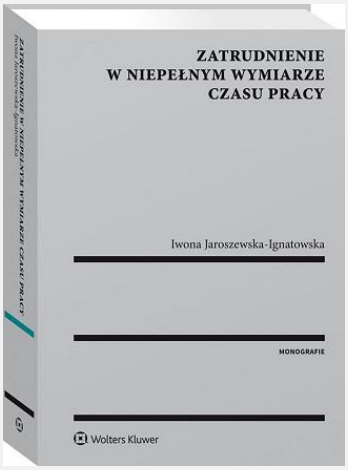
PUBLICATIONS

Part-time employment

This is the first publication on the Polish market to comprehensively cover part-time employment.

The book makes an attempt to define a 'part-time employee' on the grounds of the Polish law, as well as to determine which employee rights are applicable to part-time employees proportionally, and which ones in full.

Author:
legal advisor Iwona Jaroszewska-Ignatowska, Ph.D.



Please send your questions to
prohrevents@raczkowski.eu

Even if you outsource activities that overlap with the duties mandated by the GDPR, the recently-passed Personal Data Protection Act mandates that the President of the Personal Data Protection Office must be notified of the appointment of a personal data protection officer, including their first and last name and email address or phone number. The GDPR grants the data protection officers a high degree of independence and freedom, by making it difficult for the employers to dismiss them or to hold them accountable. At the same time, the data protection officer should be informed of all the matters related to personal data, invited to meetings and consulted on current issues, and his or her judgements should not be influenced. The employer must justify any actions that contradict the officer's recommendations. If we add to this the outlays on setting up the position and the potential conflict of interest, the possible advantages may turn out to be lesser than the risks.

Email surveillance and other forms of employee surveillance: required changes to internal regulations

Until now, this issue has not been regulated, and employers followed the recommendations of the General Inspector of Data Protection, the doctrine and the case law. Starting on 25 May, the issue is regulated in the Labor Code in considerable detail.

In the light of the new provisions, you will be able to carry out video surveillance, email surveillance and other forms of surveillance. Email surveillance, as well as other forms of surveillance (with the exception of video surveillance) will be possible if it is necessary to ensure that the employers use their working time to perform their duties to the fullest extent possible, as well as to ensure that they make appropriate use of the working tools entrusted to them. The use of video surveillance will be allowed if it is necessary to ensure that your employees, assets or the production process stay secure, or in order to maintain confidentiality of secrets which, if disclosed, could expose you to the risk of losses. The purposes, the scope and the manner of application of video surveillance should be determined in work regulations (unless you are a part of a collective labor agreement), or in an announcement if you are not obligated to issue work regulations. You must notify your employees of the introduction of surveillance at least two weeks prior to launching it. This does not apply in the situations where surveillance is already being conducted. If you do not have such regulations, they should be implemented as soon as possible; if such regulations are already in force, I recommend reviewing them for compliance with the new laws. Independently of what has been discussed above, you should inform new employees of the use of surveillance before they are admitted to work.

trainee advocate
Marta Zalewska

Candidate consent as the basis for data processing

Ronald Wasilewski
lawyer

The data processing consent of a candidate in a recruitment process should be voluntary and informed. While obtaining personal data from the candidate, the controller should supply all the information included in Art. 13 of the GDPR, including, inter alia, the identity of the controller and the purposes of data processing. If the candidate's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. It should also be remembered that consent can be withdrawn at any point without any negative consequences. You should review your consent clauses and make them GDPR-compliant where necessary. However, you should also remember that if there are other grounds for personal data processing, e.g. its necessity for the conclusion of an agreement or the controller's legitimate interests, it is not necessary to obtain an additional consent.

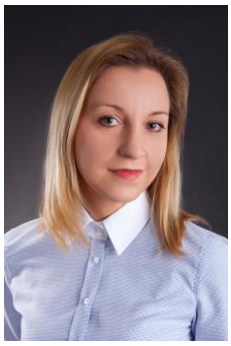
The grounds for and the course of inspections under the new personal data protection regulations

In the new Personal Data Protection Act, the legislator pays considerable attention to inspections of compliance with personal data protection laws (both the GDPR and the national industry-specific regulations). The inspection may not last longer than 30 days. It can be launched based on an inspection plan approved by the President of the Personal Data Protection Office, on the information obtained by the President or as a result of the routine monitoring of GDPR compliance. The entity that is subjected to the inspection will have to designate an authorized representative in writing.

The inspectors' rights will include, inter alia, access to the workplace being inspected between 6.00-22.00 (without a prior warning), access to all the documents and information covered in the scope of the inspection, inspecting the IT systems and interviewing as witnesses all the persons who may have information of importance in the given case. They will also have the right to interview the employees of the entity being inspected. You are required to provide conditions and means that are necessary for the inspection to be carried out efficiently. This duty encompasses, inter alia, the preparation of copies or printouts of documents that are in your possession at your own cost. If the inspectors encounter resistance while carrying out the inspection, they will be able to request the assistance of the police. The inspectors will also have the right to record the course of the inspection. The inspection will be concluded with a protocol. If you disagree with it, you will have the right to file written objections. However, the response to the objections could include further inspection. A good solution is to prepare and implement a procedure in the event of an inspection.

trainee legal
advisor Adrian
Szutkiewicz

Liability for violating the provisions of the GDPR



legal advisor Paulina Zawadzka-Filipczyk

The sanctions that can be imposed on the data controller and processor for the violation of personal data protection rules are exceptionally severe. First, nonfinancial corrective actions may be imposed by administrative order, as well as financial fines (independently of each other, i.e. both). The corrective actions include in particular: a warning, an order to bring processing operations into compliance with the provisions of the GDPR, or a temporary or definitive limitation including a ban on processing. In turn, the cap on financial fines that can be imposed for the most severe violations of the GDPR is 20,000,000 million euro, and in the case of an undertaking, 4% of its worldwide annual turnover for the preceding financial year (the higher amount applies).

The Raczkowski Paruch personal data protection team

is a team of lawyers with many years of experience in personal data protection who will comprehensively prepare your company for legally compliant personal data processing.

legal advisor Dominika Dörre-Kolasa, , Ph.D.

legal advisor Edyta Jagiełło

legal advisor Daria Jarmużek

trainee legal advisor Grzegorz Larek

trainee advocate Jakub Lasek

legal advisor Paweł Sych

trainee legal advisor Adrian Szutkiewicz

trainee advocate Paulina Szymczak-Kamińska

trainee advocate Marta Zalewska

Ronald Wasilewski lawyer

legal advisor Paulina Zawadzka - Filipczyk

Ius Laboris Poland Global HR Lawyers
Raczkowski Paruch