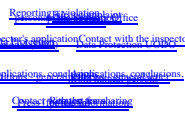


Enter the phrase you are looking for



Office helpline 606-950-000

President and Office

Right

Education

Cooperation

Tutorials

contact

Complaints

» [Top topics](#) » Administrator » Complaints

Data Protection Officer

How controllers should handle data breaches

The lack of access by the administrator to personal data is also a breach of protection data - this is one of the reminders contained in a special information material UODO regarding this issue.

From May 25, 2018 to May 25, 2019, administrators, fulfilling the obligation resulting from art. 33 paragraph 1 of the General Data Protection Regulation (GDPR), reported 4 539 breaches of protection to the President of the Personal Data Protection Office personal data. Two-thirds of the notifications came from administrators from the private sector and one-third from public sector administrators.

In the case of the private sector, the largest number of applications came from companies: telecommunications, insurance, financial, banking and services health. In the public sector, notifications of incidents with personal data the most frequent submissions were local government units, schools, kindergartens and nurseries and health care facilities.

Our annual experience in the field of receiving and analyzing notifications of personal data breaches shows that controllers continue to have difficulties assessing the risks to the rights and freedoms of data subjects they may pose a given event or whether it is a breach of data protection at all, as provided for in Art. 33 GDPR. And this is the case, for example loss of access to the data being processed. However, such a situation may arise when the system is infected ransomware virus that encrypts, for example, access to entire databases, and sometimes their backups.

All incoming data breach reports are scrupulously analyzed, and when there is a need to obtain further ones information - the Personal Data Protection Office establishes quick, often also by phone, contact with administrators and their designated security inspectors data.

Meetings with other expert entities, such as CSIRT NASK, also serve to exchange experiences and information as well as improve practices in the field of detection and prevention of violations related to IT infrastructure.

Our experience from the first year of application of the GDPR provisions in the field of personal data breaches and developed Based on these experiences, we have included guidelines for data controllers and data protection officers in a special material entitled "Responsibilities of controllers related to personal data breaches", available below. We have I hope that it will be helpful in improving administrators' practices in this area.

2019-05-30

Attached files

[Administrators' obligations related to personal data](#)

