ZFODO

Breaches in personal data protection 2020

The Report od ZFODO – Association of Personal Data Protection Companies

00

About the report

- The study covered **454 organizations** supported by companies united in the ZFODO between **May 2019 and May 2020**.
- The above-mentioned organizations include both the public and the private sector.
- The above-mentioned organizations were supported by companies united in the ZFODO, which operated either in the field of DPO outsourcing or cooperated in other permanent ways in the personal data protection area.

4ITSECURITY AURACO Discretia ENSI KANCELARIA EKSPERTÓW FORSAFE BEZPIECZEŃSTWO PONAD WSZYSTKO iSecure

JDS CONSULTING LEX ARTIST ODO 24 ODO MANAGEMENT GROUP OMNI MODO EKSPERT W DZIEDZINIE OCHRONY DANYCH OSOBOWYCH Orleccy bezpieczeństwo i edukacja

Partner wspierający CYBERTEQ®

01 Introduction

We are proud to present you the latest report on breaches in the personal data protection area, which has been prepared by the ZFODO. The main goal of the report is to make you familiar with the key issues related both to the occurrence of these breaches and to the professional support they require.

The report is based on true data covering breaches, which have been managed by professionals operating in the personal data protection area, that is by the members of the ZFODO. It is a compilation of statistical data, processed to be fully anonymous, which guarantees that particular cases of breach cannot be identified. The analysis of statistical data enables to identify trends and may change the attitude of entrepreneurs to the problem of breaches. We encourage you to read the report and learn the conclusions of our experts in detail.

According to our data, the risk of a breach is present in any business field. Regardless of the business area, the entrepreneurs remain uncertain what responsibilities they have in case a breach has been identified. These doubts are fully justified, because performing tasks resulting from the GDPR properly requires professional knowledge combined with a wide experience of the matter.

Acquiring the knowledge you need forces specialization of the company staff, which usually means investing large amount of money in creating new positions, such as the data protection officer. Additional costs result from numerous professional trainings of employees in charge of managing breaches.

Gaining the sufficient level of experience requires a lot of time, as breaches do not occur frequently. Statistical data show that an average data controller deals with a breach 0.65 times per year, which is an insufficient number to become a professional. Nonetheless, a mistake made while dealing with a single breach may have a detrimental effect on any entrepreneur running a business.

A potential solution of the above-mentioned problems is to outsource this area to the professionals operating in the field of data protection.

Outsourcing it enables an easy and economical access to high-class specialists who require the necessary experience and deal with the breaches of personal data on a daily basis. Only such specialists guarantee, they fully recognize the needs of an entrepreneur, who seek effective and proven solutions, ready to be implemented within 72 hours after identifying a breach.

One cannot forget the best solution is fixing the reasons instead of curing the symptoms. We therefore advise to identify the business risk related to a potential breach in advance. A reasonable entrepreneur should make sure, that the area of data protection is supported by a qualified personnel. The choice between outsourcing this field or appointing an employee to be in charge with it remains individual, depending on many business factors.

02 Probability of breaches

297
Number of recorded breaches

454
Total number of organisations

0.65
Average number of breache per organisation

- The report covered 454 organizations, supported by 9 different companies (all of which are associated in the ZFODO) operating either in the field of DPO outsourcing or cooperating in other permanent ways in the personal data protection area. Between 25 May 2019 and 25 May 2020 the total number of officially recorded breaches in these organizations reached 297.

This gives an average of 0.65 incidents per year for each organization. The survey is based only on these incidents, which were reported to the above-mentioned companies by the organizations they support. Thus the real number of breaches may be higher.

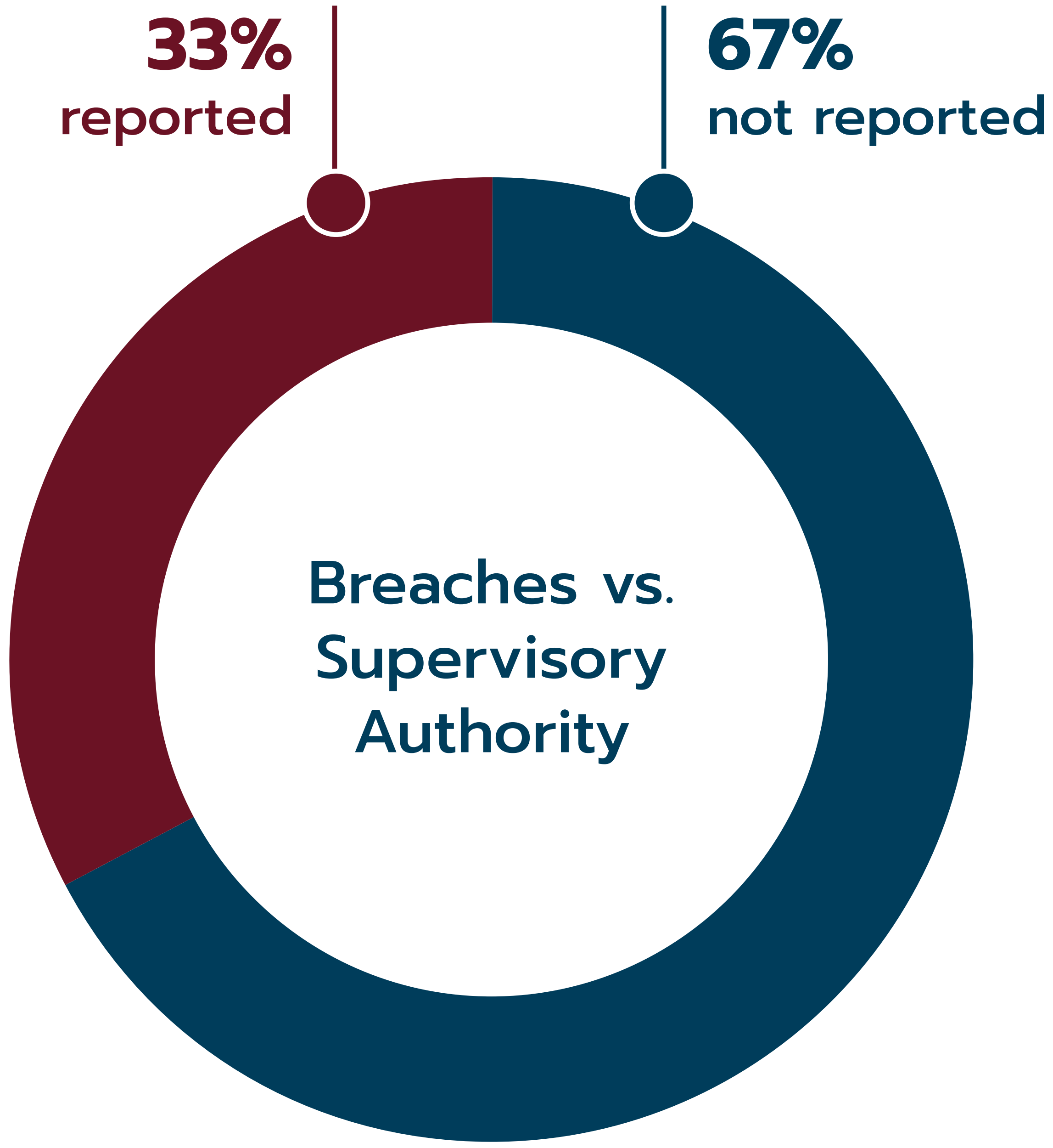
Tomasz Osiej
OMNI MODO SP. Z O.O., CEO

Compared to the previous study (2018 -2019), the present one is more detailed and, one can say, more mature. It is because not only the ZFODO but also its members have developed during the period under review. Therefore, instead of the previous 277, the current data covers 454 organizations.

The next reason is the raised awareness related to qualifying certain events as breaches and to the necessity of reporting them. You may say that administrators are consciously more courageous. All this has caused an increase in the average number of breaches per organization from 0,46 to 0,65. This difference may not seem so spectacular, but it reflects a stable growth. As data administrators under the GDPR each day we get to understand our role better and better. We are still learning what should be typed as breaches, how to evaluate them and finally, which ones should be reported and to whom.

In the summary of the previous report we predicted that the breach rate would be increasing, which has been reflected in the current research. Apart from the raised awareness there are obviously many more factors influencing this trend, such as the development of the companies under study, the further digitalization of their processes, probably also the difficult COVID-19 time, which has also been covered by the study. But in my opinion the raised awareness was nonetheless the deciding factor.

03 Incidents reported to the Supervisory Authority



- **Nearly 70% of breaches have not been reported to the Supervisory Authority. Pursuant to Article 33(1) of the GDPR, a breach may not be reported to the Supervisory Authority if it is "unlikely to result in a risk to the rights and freedoms of natural persons".**

Assessment of probability of violation of rights or freedoms raises difficulties and concerns for the administrators in many situations.
For comparison, in the last year's study, 59% of breaches were not reported to the Supervisory Authority.

Maciej Kaczmarski
ODO 24 SP. Z O.O., CEO

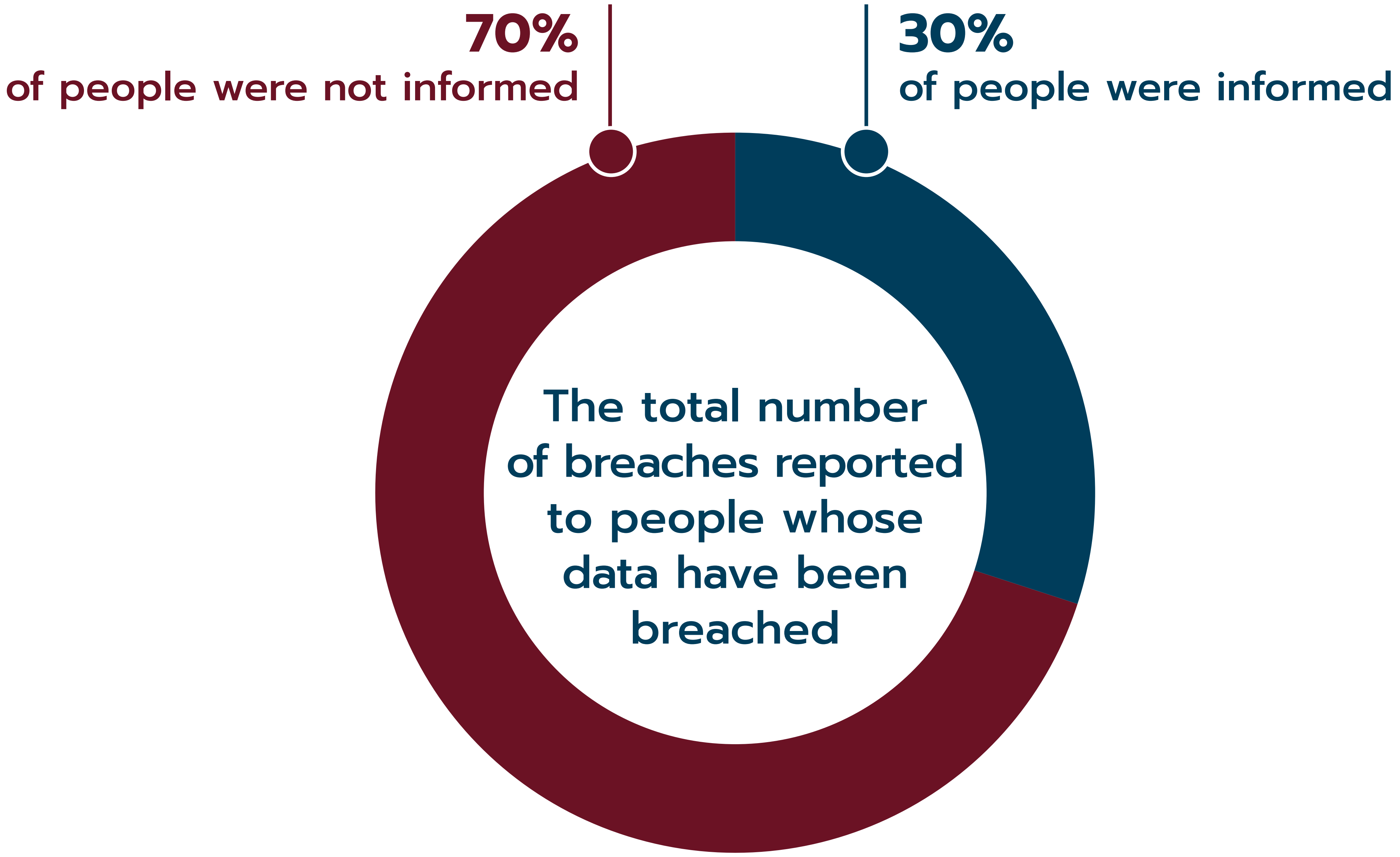
The latest data indicate an increasing trend of breaches which have not been reported to the Supervisory Authority. Each case requires an individual and thorough analysis, however, administrators should be aware that a decision not to report a breach may be risky in the long run.

The key issue is to correctly identify the situation in which notification is the best solution. The next step is to organize the notification process itself properly. The process requires the involvement of legal experts who will prepare the documentation and fill in official forms. In most cases it requires the participation of IT experts, who will ensure the implementation of security measures minimizing the risk of a recurrence of a breach, and will also help to conduct the relevant risk analysis documenting the correct choice of implemented solutions.

Administrators reporting breaches are under time pressure (72h) and it is not difficult to make a mistake, e.g. they may describe the breach insufficiently, they may superficially indicate the consequences for the people affected by the breach or incorrectly estimate the probability of violating their rights and freedoms. The consequence of such a mistake may be, for example, a further investigation by the Supervisory Authority.

04

Incidents reported to data subjects



- **Regardless of the notification of the breach to the Regulator, pursuant to article 34 of the GDPR, "If the breach of personal data protection may result in a high risk of violating the rights or freedoms of natural persons", we should also inform the affected persons about it.**

As in the case of reporting breaches to the Regulator, the assessment of a high risk of violation of rights or freedoms raises difficulties in interpretation.
In the previous study, the breach was not reported in 76% of cases.

attorney Konrad Wysocki

JDS CONSULTING SP. Z O.O. SP. K.

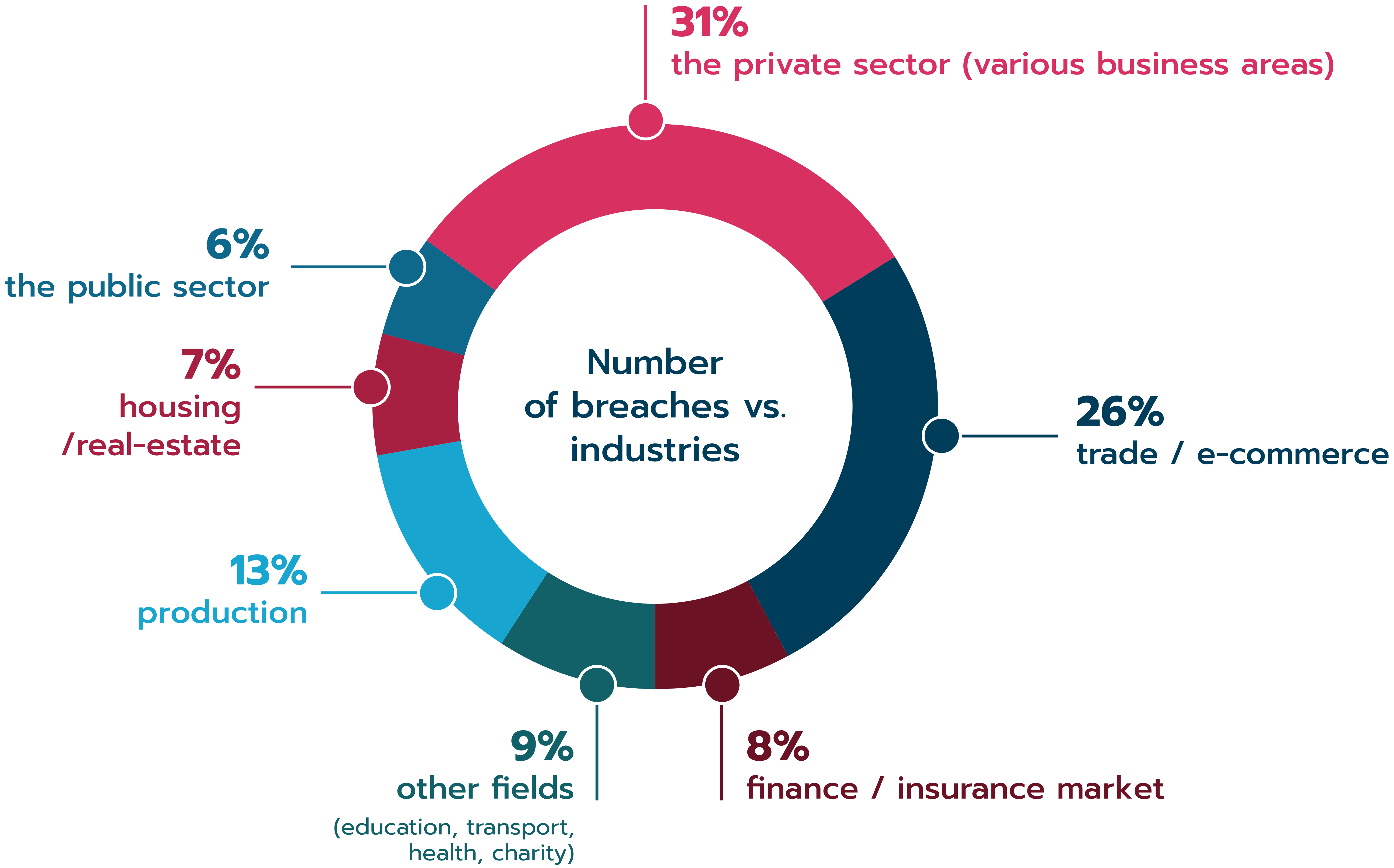
Identifying a data protection breach by a data controller does not only lead directly to all consequences resulting from the possibility of imposing an administrative penalty by the supervisory authority. In case of a breach, the GDPR imposes additional notification obligations on data-processors. These obligations are practically unknown in any other legal act present in the European law.

The existence of a breach usually requires cumulative occurrence of the three following premises:

1) *The breach must concern personal data which were sent, stored or otherwise processed by the entity affected by the breach.*
2) *The breach may result in destruction, loss, modification, unauthorized disclosure or access to personal data.*
3) *The breach is the result of not following the data security principles. Each data controller is required to notify the breach to the supervisory authority without undue delay and, if possible, no later than 72 hours after the breach has been identified, unless the controller is able, in accordance with the principle of accountability, to demonstrate that the breach is unlikely to result in a risk to infringe rights or freedoms of natural persons.*

The element that enables proper breach management and assessment is the legal awareness in a given organization, the development of which should be taken care of by the designated data protection officer.

05 Industries most exposed to the risk of personal data breaches



- The private sector generated the vast majority of all breaches recorded by the ZFODO. However, this should not lead to drawing too far-reaching conclusions. The particularly strong presence of the private sector may also indicate that the ZFODO member companies serve mostly the private sector.

It is worth noting that industries such as e-commerce and finance/insurance generated 35% of all breaches (previously 30%).

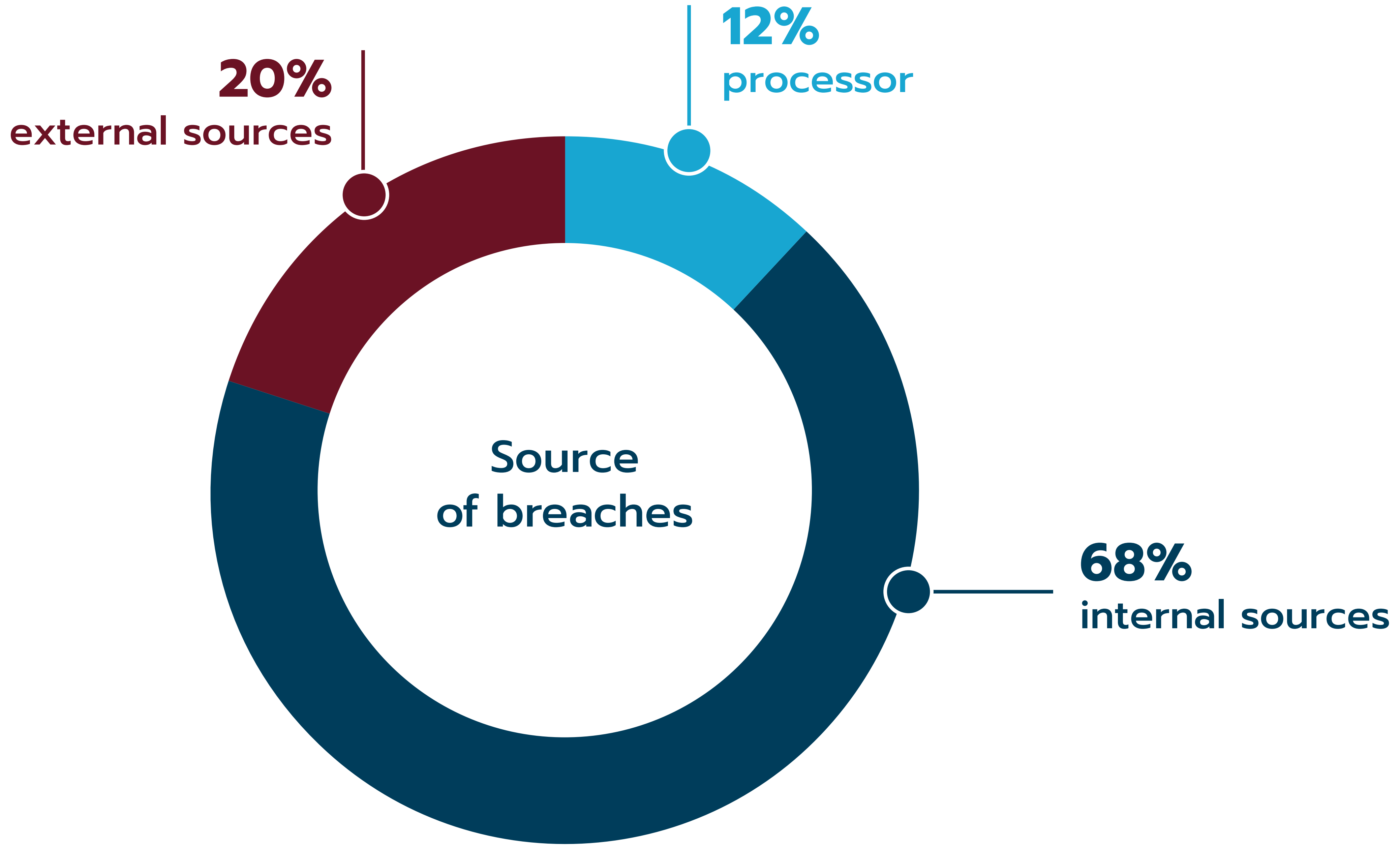
Piotr Kawczyński

FORSAFE SP. Z O.O.,MANAGING DIRECTOR

In the analyzed period of time, we observed an increase in the number of breaches in the private sector, with particular participation of entities specializing in electronic commerce, which could probably be related to the consequences resulting from the case of morele.net. Administrators from this sector have reported violations, both these qualifying indisputably as well as those whose evaluation was on the verge of being notifiable in PUODO. It could have been due to fear of penalties, but in my opinion in most cases the basic argument deciding about the notification was an independent assessment by the authority and leaving the decision to the President of the Personal Data Protection Office.

In the rest of the private sector, the overwhelming number of breaches and breaches were related to the loss of data confidentiality through unauthorized disclosure of personal data - the source of these behaviours were system errors and unintentional human activity.

06 Source of personal data breaches



We decided to divide the sources of breaches into 3 categories:

- External - not related directly to an organization: hackers, former employees etc.
- Internal - employees and associates of an organization.
- Processor - entities processing personal data at the request of the Data Controller within the meaning of Article 28 of the GDPR

The vast majority of breaches were caused by the actions of employees or associates of an organization.

Michał Geilke

DATA PROTECTION OFFICER, OWNER OF ORLECCY - SECURITY AND EDUCATION

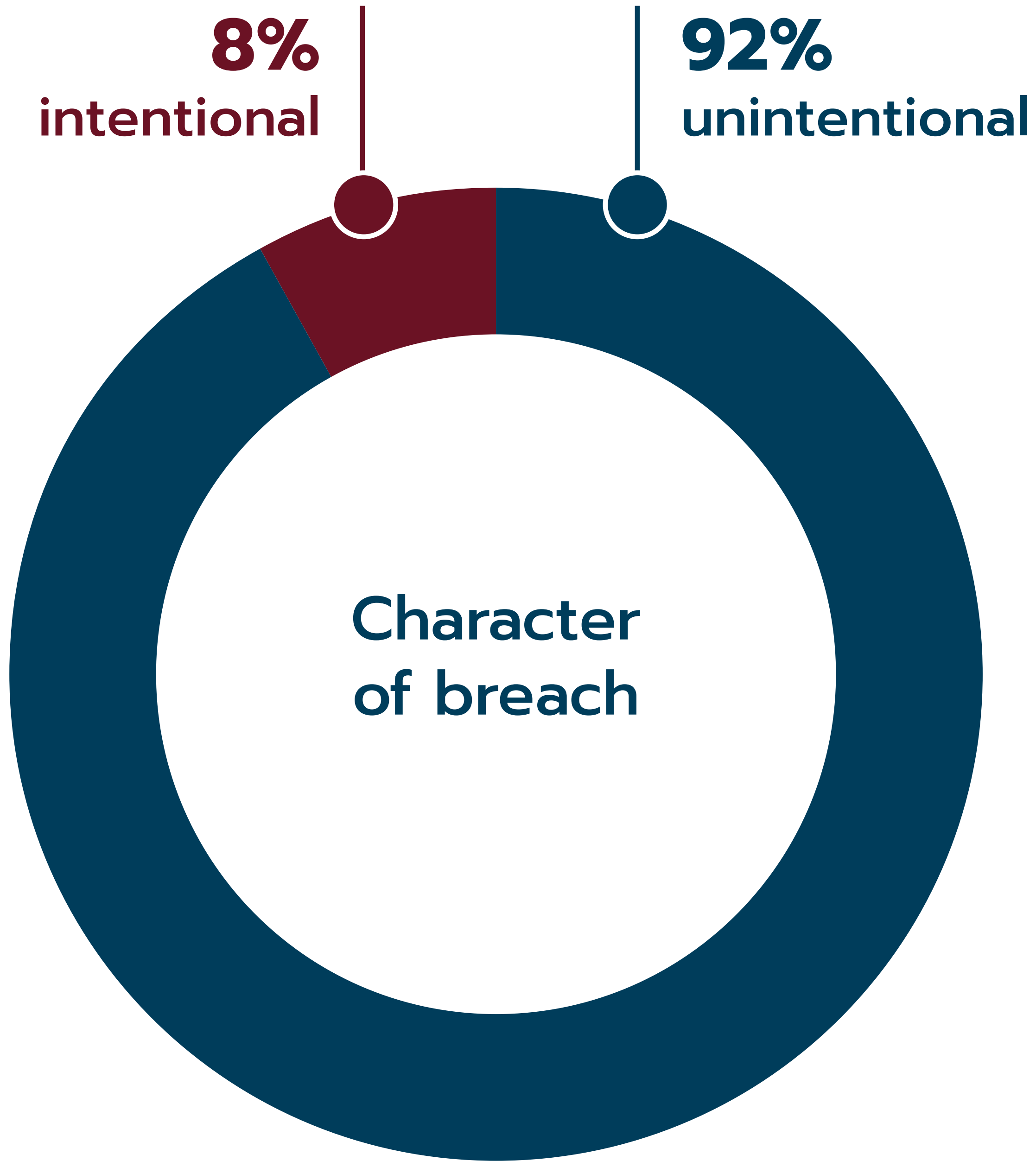
The obvious remark of Kevin Mitnick that "humans are the weakest link in the security chain" still remains a huge problem in all personal data processing. Moreover, apparently "only people who do nothing make no mistakes". So the reason we are at work is to perform a specific type of order or task. If the task involves the processing of personal data, the risk of making a mistake with serious consequences for the entire organization unfortunately increases.

Although it is the data controller who decides on the purposes and methods of personal data processing, these activities are actually performed by a specific employee or subcontractor. In turn, the Data Controller is, in principle, responsible for any mistake of the employee or subcontractor in the first place. In our opinion, the indicated dependencies determine the fact that most threats and breaches are of a personal character - their source are employees of the data controller.

An important element of security is therefore building the awareness of employees and subcontractors about the categories of personal data with which they work, as well as the threats and risks associated with them.

Such risks can be minimized, in particular through appropriate training, but also through proper planning of the working day (haste makes waste) or creating appropriate provisions in contracts with employees and subcontractors.

07 Intentional vs. unintentional character of breaches



As many as 92% of breaches are acts of negligence (in previous research – 89%). The examples are:

- incorrectly addressed emails,
- failing to use BCC (Blind Carbon Copy),
- sending traditional mail to a wrong postal address (sharing someone else's personal data).

Intentional acts included:

- stealing a laptop (or other data storage devices),
- phishing scams,
- access to personal data by unauthorised individuals.

Michał Sztąberek
iSECURE SP. Z O.O., CEO

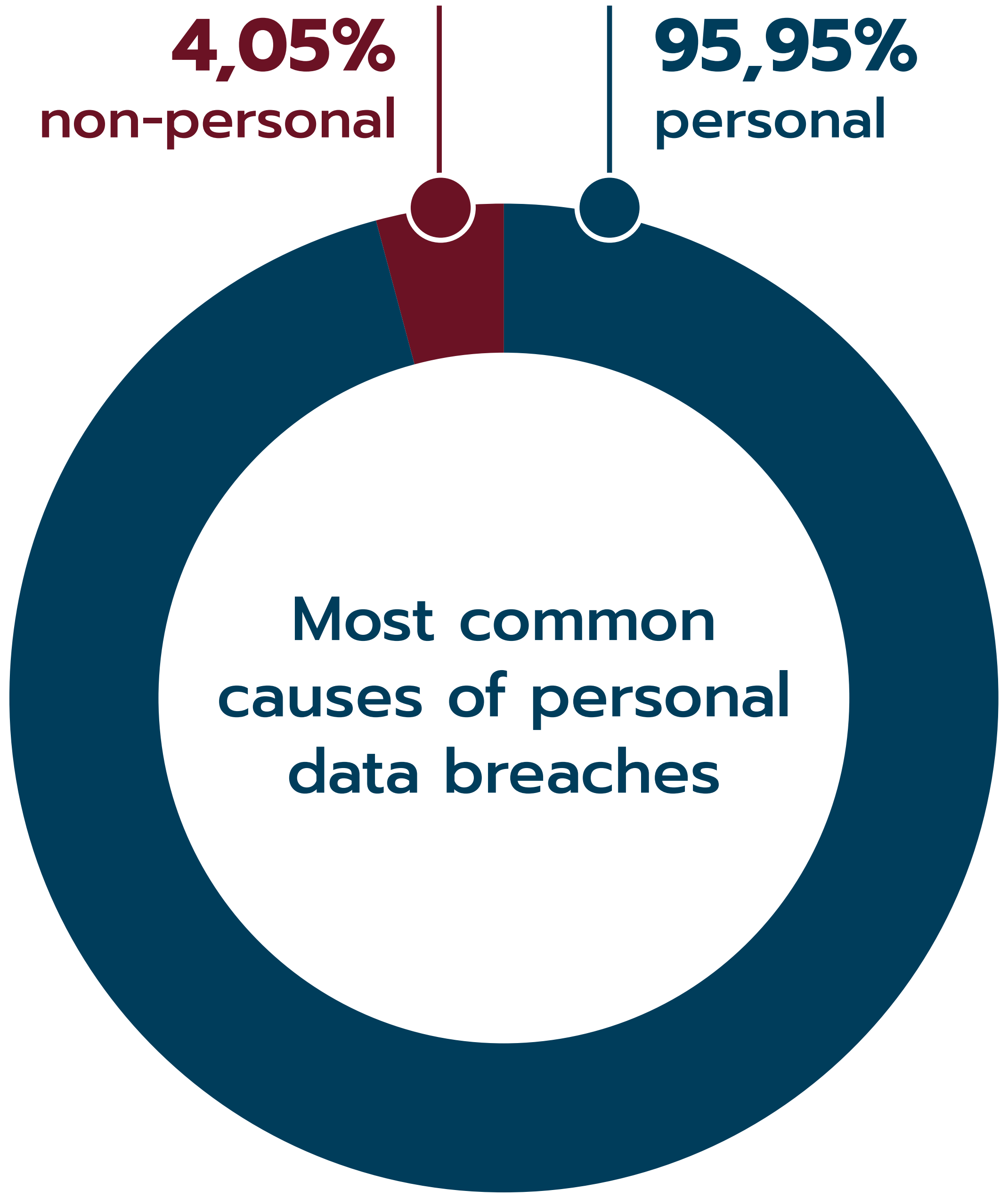
To be honest, I am not surprised that the vast majority of breaches were acts of negligence. My professional experience shows that the most common problem is... sending e-mails. Electronic mails with personal data, which are either attached or revealed in the content of a message, are being sent to the wrong recipients, which results in a loss of confidentiality for the data subjects.

The good part, if any, is that an employee is aware of the fact that this kind of notification must be reported to organisation&#39;s data protection officer (DPO), so that legal proceedings can be started (the remedial action – in agreement with managerial staff, notifying the Personal Data Protection Office – if it is necessary due to the risk of violation of personal rights and freedom).

Unfortunately, remedial actions aimed at preventing similar breaches in the future are the biggest problem. Another training can be less efficient, but I underline it is still worth doing (especially when it focuses on breaches similar to the ones which occurred in a given company. This can make employees become more careful in the long run).

What is more, I strongly recommend implementing data breach prevention tools. The only way to radically minimize the risk of breaches is an approach combining procedures, training courses and technical measures.

08 Personal vs. non-personal causes



- **The personal reasons are related to the so-called human factor. Thus, both deliberate actions of external persons (e.g. hackers) and unintentional mistakes of the employees of a given organization.**

Non-personal causes are situations where a breach was caused by malfunctioning technology, situations beyond the control of human will.
In the previous study, the distribution was as follows: 89% - personal causes, whereas 11% - non-personal causes.

Przemysław Zegarek
LEX ARTIST SP. Z O.O., CEO

The result of the study is a warning to all those who believe that new technologies will protect the information we have in a maintenance-free manner. Working with people is tedious, requires regularity and consistency. And it does not guarantee success. However, this is the only way to eliminate as much as 96% of breaches which occured in the surveyed organizations!

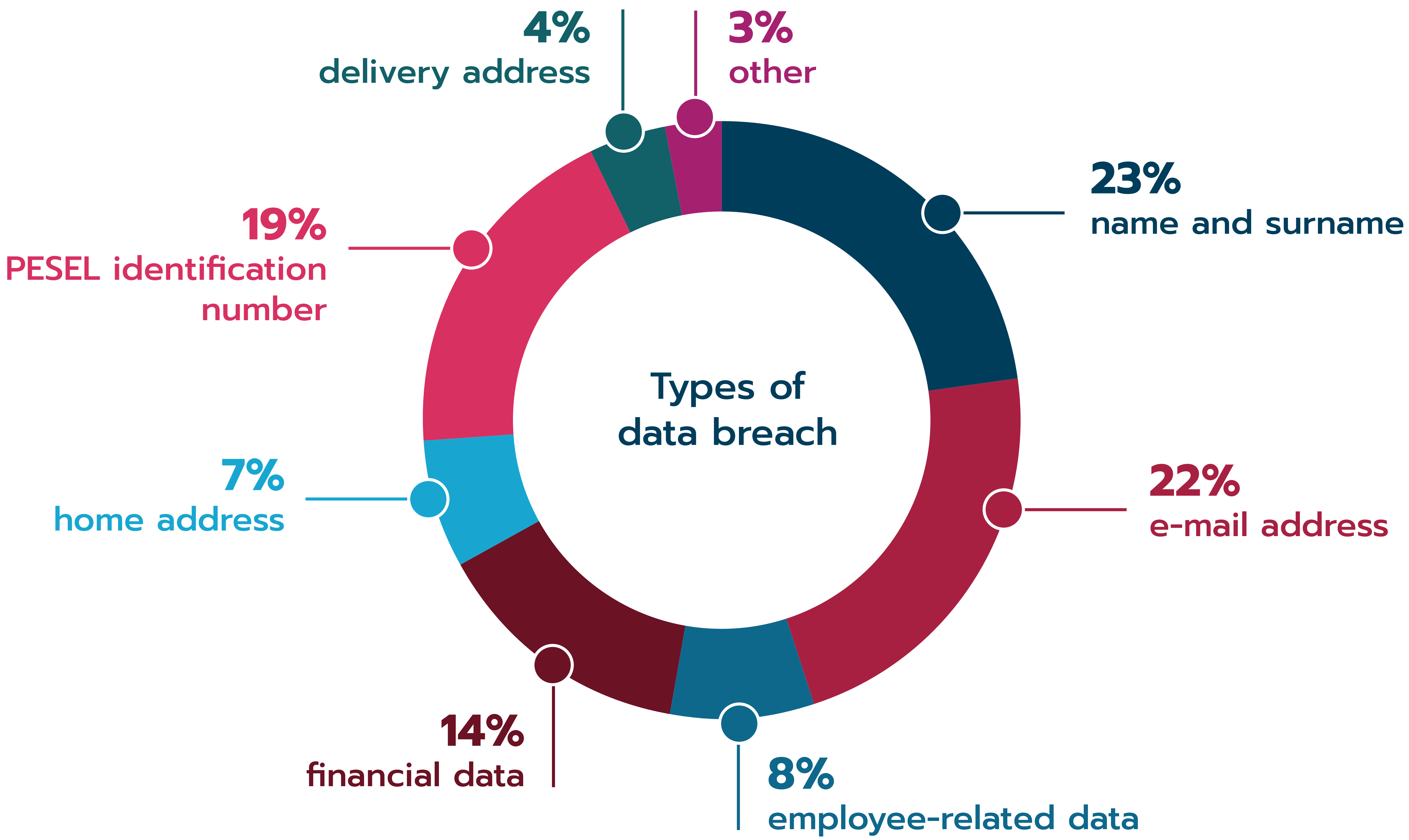
We are still learning to work with people. We improve trainings, create tools to diagnose the level of GDPR awareness. When I look back at our approach to training or collaborating with people 5 or 10 years ago, I see a huge change and progress.

Compared to the human factor, technology fails rarely.

The key to safety lies in a smart way of working with people, supported by the best technology.

09

Most frequent breaches per data category



The graph illustrates the categories of personal data that have been most frequently breached.

The specific subdivision of categories is the outcome of the actual scope of the data, which has been revealed in a variety of data breach reports. The indicated data categories have been grouped and summed in order to help identify those being the most common victims of the breaches in question.

Magdalena Chmielewska

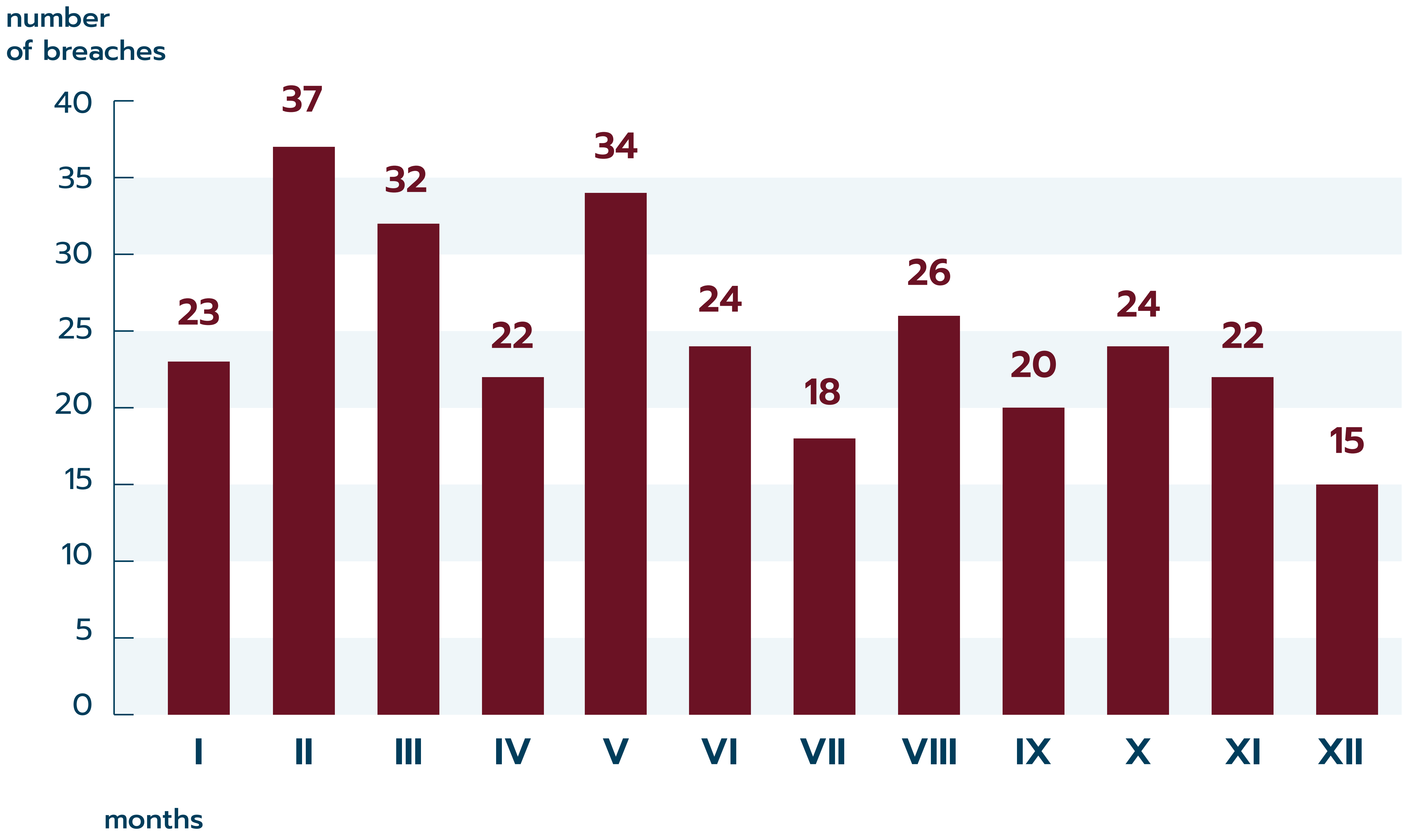
ODO MANAGEMENT GROUP SP. Z O.O., CEO

Under the current GDPR laws, it is necessary to differentiate between two categories of personal data: ordinary personal data (processed under Article 6 (1) of GDPR), and special categories of personal data (processed under Article 9 (2) of GDPR). The processing of special categories of personal data (e.g. data concerning health) implies the need to meet a variety of other – higher requirements as far as safeguarding the protection of such data is concerned. Each instance of their breaching may result in a major risk of infringing the fundamental rights and freedoms of the data subjects.

The breaches of personal data identified at the turn of 2019 and 2020 – just as in the previous year (between May 2018 and May 2019) – typically concern ordinary personal data, i.e. a person's first name and surname (23 percent), or their e-mail address (22 percent). In as many as 20 percent of the breaches under study, a breach was found related to a person's PESEL identification number. Although the PESEL identification number has been classified as ordinary personal data, breaching the principle of confidence of this number, particularly in combination with other data (e.g. one's first name, surname, or home address) may result in numerous threats, e.g. an attempt of committing a credit fraud, an insurance fraud, claim allowances that a data subject is not eligible for, or deprivation of data subject's civic rights.

The latest report shows that the scale of financial data breaches has declined 15 percent in comparison to the previous period, which can indicate both a potentially higher level of awareness of the holders of such data and also a variety of more effective types of security measures applied by different entities.

10 Data breaches vs. months of year



- The chart shows the number of personal data breaches broken down by months when they were recorded. A cyclical survey repeated over several years will allow to detect trends in the number of breaches or to identify the months most prone to data breaches.

Tomasz Gwara

DISCRETIA SP. Z O.O., PARTNER, CEO

Most personal data protection breaches occurred in the summer and early fall, which was followed by a decline. It is similar to the trend observed last year. How to explain this cyclicality? It may reflect the increased business activity of companies in the second and third quarter of the year.

Observing the data leads to yet another conclusion: the overall number of breaches is not decreasing and there is no month when no breaches would be reported. This means that companies are still developing their competences in the field of personal data protection - they are still not able to effectively counteract breaches, but at least they report them more effectively.

We also recommend that you read the positions and opinions of the ZFODO:
www.zfodo.org.pl/opinie/

We respond to any practical problems posed by our clients.

ZFODO

Związek Firm Ochrony
Danych Osobowych

Ul. Hoża 86/410,
00-682 Warszawa

e-mail: kontakt@zfodo.org.pl
www.zfodo.org.pl