Your World First

C/M/S/
Law.Tax

Amendments to the EU personal data protection law – new challenges and opportunities for business entities

Report prepared by CMS
First opinion poll in Poland

July 2016

General Data Protection Regulation

4 May 2016 – publication of the new law

25 May 2016 – effective date

Time for adaptation: 2 years

Concerns: all business entities operating on the territory of the European Union

New process in the company:
Evaluation of the impact on privacy

25 May 2018 – the new law will be enforced starting from this date

Penalties for failure to adapt: up to EUR 20 million or 4% of the global annual turnover in the preceding financial year

Table of Contents

Greater protection, new opportunities

All businesses operating in Poland will need to adapt their activity to the new EU law – the General Data Protection Regulation that will be applicable starting from 25 May 2018.

The most important conclusions drawn from reading the regulation can be narrowed down to two principal theses. First, the protection of privacy is recognised by the EU legislator as the fundamental right of each data subject and the role of the supervisory authorities is to maximise such protection by means of broad prerogatives arising from the new regulations.

Second, the regulation creates new opportunities for undertakings to process data for business purposes – for example by precisely indicating how to lawfully profile customers e.g. in order to grow sales. It also responds to difficult questions including how to process children's personal data or how to evaluate the impact of data processing on the activity carried out.

Is the business ready for such a profound change of regulations? We have asked about this in our survey. The results presented in this report are accompanied by essential information for businesses regarding the changes in the law, their significance and what must be done to be in compliance with the new regulation.

Enjoy the read!

r.pr. Tomasz Koryzma
Partner
T +48 22 520 8479
E tomasz.koryzma@cms-cmck.com

r.pr. Marcin Lewoszewski
Senior Associate
T +48 22 520 5525
E marcin.lewoszewski@cms-cmck.com

Business and the new regulations

The new EU data protection regulations entail new obligations for companies and an intensive preparation period. Are businesses ready? How much do they know about the amendment?

A report on the awareness of Polish businesses as regards the changing data protection regulations, what these changes mean, and how companies plan to react to them is presented on the following pages.

The report is based on data from an original survey carried out from April until May 2016 among representatives of over 100 companies operating in Poland in sectors that will be most affected by the changing regulations.

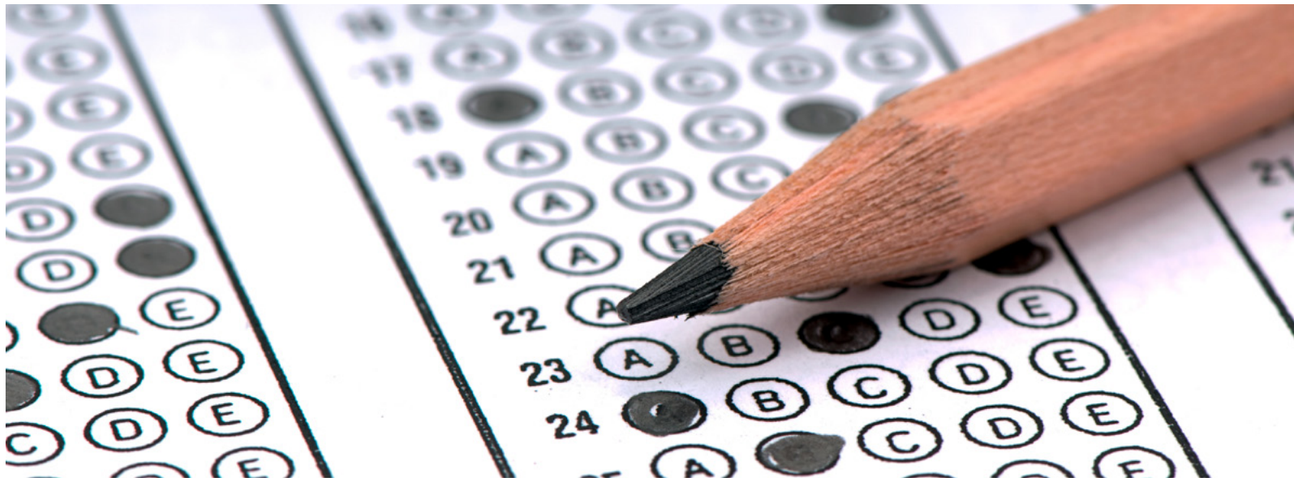
Nearly half of the respondents (48%) work in companies with over 500 employees and 68% are employed in international corporations.

The following sectors enjoyed the strongest representation: insurance (19%), banking (14%) and technological (11%). Many of the respondents work in the FMCG, telecommunications, automotive and e-commerce sectors.

Respondents were mainly management board members and department directors and managers. The majority of them work in the legal (29%) and IT (11%) departments, followed by representatives from the compliance, security, sales and marketing departments.

We have divided the conclusions from the survey into four chapters:

I. Change awareness
II. Awareness of the consequences
III. Planned activities
IV. Perception of the situation

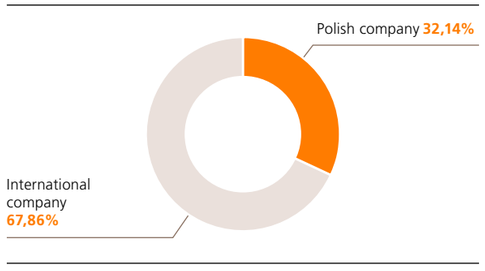


CMS survey participants:

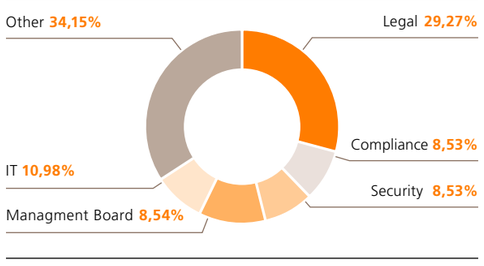
Number of employees

Industry / sector the company operates in

Company's footprint



Department in which the respondent is employed



I. Change awareness

The result of the survey confirms that the vast majority of businesses are aware of the upcoming changes in the EU personal data protection law. Considering the scale of such changes, it is a positive phenomenon.

At the same time, as the survey results may suggest, the knowledge about the essence of the new regulation and its impact on business operations is rather superficial.

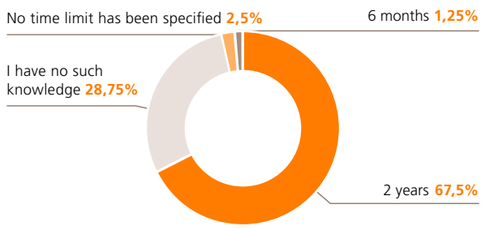
Time is already running

The vast majority of businesses already know about the relatively short – 2-year – period provided by the EU legislator to adapt their activities to the new regulations.

> The unification of regulations will facilitate conducting business activity in the European Union
>
> *CMS survey participant*

Are you aware that in May 2016 new EU regulations on personal data protection will enter into force, imposing a number of new obligations on business entities?

Do you know how much time business entities will have to comply with the new law?



II. Awareness of the impact

Business entities correctly identify the areas of business activity which are most vulnerable to the upcoming changes. Such areas may be reduced to a common denominator: customers' personal data.

Departments such as the sales, marketing and customer service departments i.e. those that directly process customer data, were most frequently identified as the departments that require the greatest changes in connection with the new regulations. A considerable group of respondents also indicated the HR department that processes employee data.

The General Data Protection Regulation will drastically increase sanctions for failure to comply with the personal data protection regulations. The respondents rightly indicated that the potential sanctions may reach amounts that are substantial for any business entity i.e. even 4% of the global annual turnover in the preceding financial year or EUR 20 million – whichever figure is higher.

Increased costs?

The new EU regulation will significantly increase the obligations of entities that process personal data. In the respondents' view it may entail an increase in the costs of the conducted activity, at the very least due to the necessity to implement professional protection systems for the processed data or a more careful selection of entities that process data on a fee or contract basis (e.g. in accounting or IT service centres).

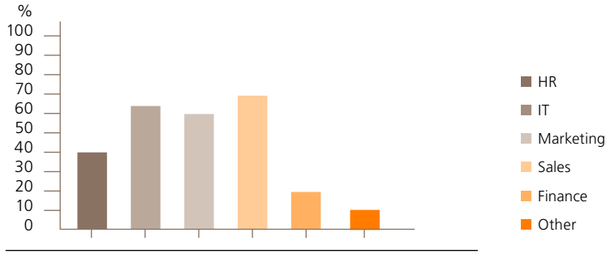
Supporters of the amendment positively evaluate the standardisation and consistency of the regulations as well as making personal data protection a reality. Sceptics express their concern as regards the potential impact of the EU regulation on the decrease of customer confidence. They believe that the regulations are too general, they impose too many obligations on companies and the necessity to provide customers with complex clauses may have a negative impact on customer confidence.

At this stage the evaluation of how the regulation will impact customer confidence may be premature as the manner of satisfying the obligations by business entities will be of key importance.

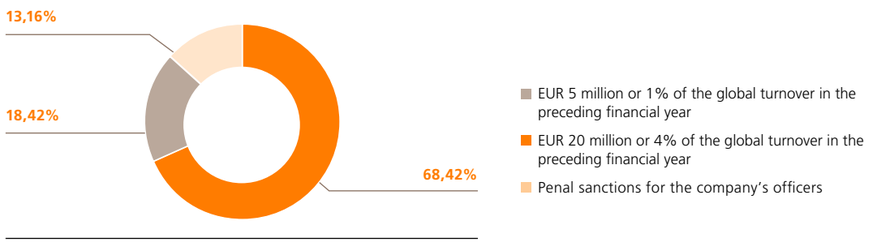
New opportunities

Only a small group of respondents perceives the new law as a growth opportunity for their business. This may mean that the use of such tools as Big Data or customer profiling is not yet common in Poland.

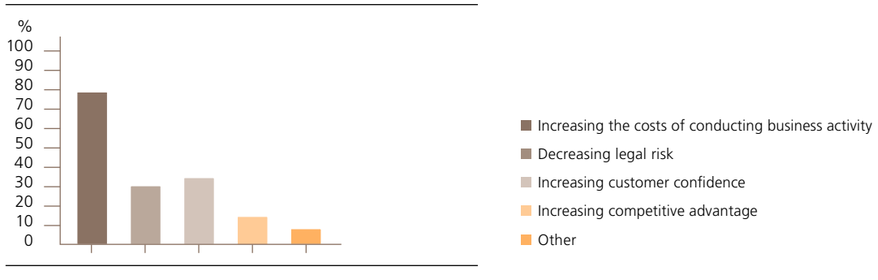
Based on your experience, which business areas require the greatest changes in connection with the new regulations?



Do you know what sanctions are provided for business entities for failing to adapt their activity to the new regulations on personal data protection?



In your opinion, the implementation of the new EU regulations on personal data protection will result in:



III. Planned activities

The business entities that participated in the survey are intensively familiarising themselves with the new regulations, however, most do not undertake further activities.

Few business entities undertook other preparatory activities such as mapping business processes that should be evaluated in terms of the new regulations. Also, few business entities decided to verify the list of service providers that have access to personal data.

Such a result may be surprising due to a number of reasons – mostly due to the fact that the new regulation will make it necessary to renegotiate agreements with such entities or will even result in ending cooperation with them. This, of course, may require incurring additional costs by the business entities.

People and systems

Similarly, the adaptation of IT systems will require numerous analyses, negotiations with the software supplier and possibly incurring costs related to the necessary modification (we would like to draw your attention to the *right-to-erasure* or *privacy-by-design* solutions adopted in the regulation). At the same time, the majority of business entities do not know whether they will increase financial or human resources for the purposes of safeguarding data.

Business entities plan to increase the awareness and knowledge of the staff – both by means of internal communication channels as well as e.g. by sending employees to post-graduate studies within the scope of personal data protection.

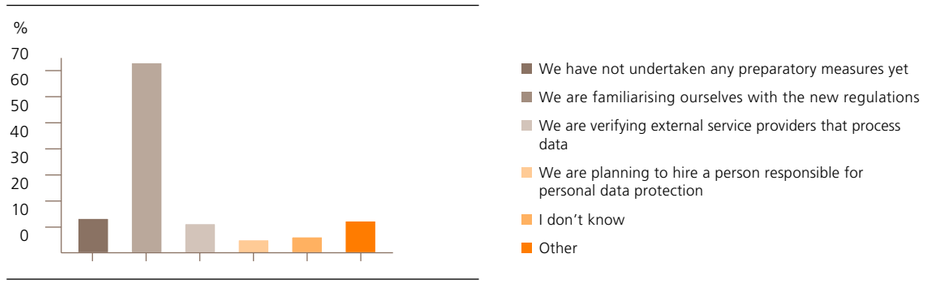
Key factors

Engaging the management board in the process of implementing new EU regulations is a highly desirable phenomenon – if only due to the significance of the new obligations and the potential sanctions. The management board should be informed about the upcoming changes and involved at an early stage in shaping the company's organisational culture as regards personal data protection.

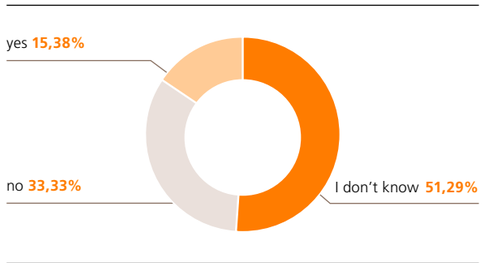
The engagement of external entities that professionally deal with adapting business operations to the new law should be assessed similarly. Their involvement makes it possible to benefit from the experience of others and to avoid their mistakes.

> We are preparing relevant procedures and policies to effectively react to violations
>
> *CMS survey participant*

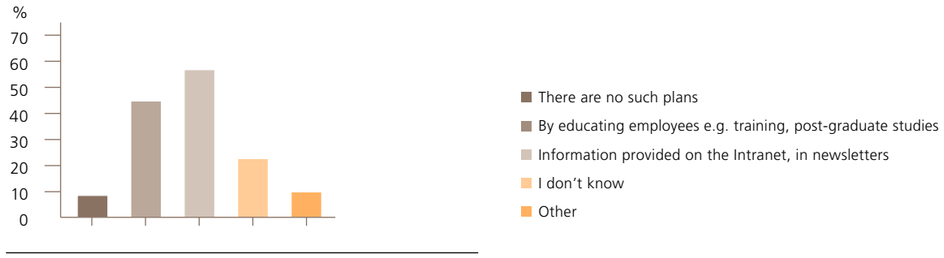
What preparatory measures have been taken so far by your company in order to adapt the conducted business activity to the requirements of the new law?



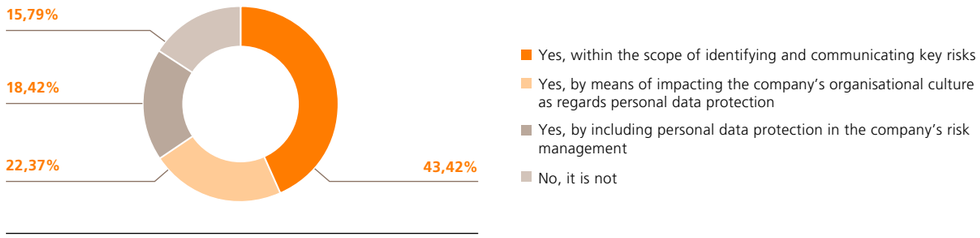
Is your organisation planning to increase resources (financial and/or human) for the purposes of protecting information, including personal data in connection with the new law?



Is your organisation planning to increase the employees' awareness of the new law, and if so, how?



Is your organisation planning to include the management board in the implementation of the new EU regulations on personal data protection?



While implementing the new data protection law, does your company intend to draw from the expertise and experience of third-party service providers?

IV. Perception of the situation

The majority of business entities that participated in the survey see the need to provide further information about the upcoming changes.

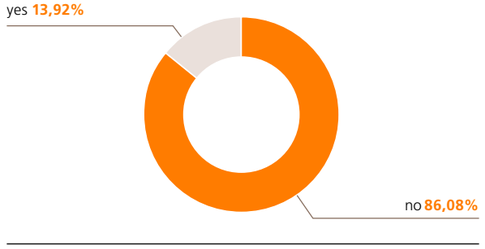
Both the Inspector General for the Protection of Personal Data (GIODO) and other entities undertook educational activities with respect to the changes, however, the level of knowledge presented by business entities still leaves a lot of room for improvement. This could be because in Poland the amendments to the Personal Data Protection Act, e.g. in connection with holding the function of the information security administrator, were developed at the same time as the EU regulation. Hopefully, more intensive education will be carried out in the near future.

It pays to be compliant

The vast majority of business entities agree on why it is worth observing the new regulations: mostly due to the financial risk, possible sanctions as well as reputational risk.

On the other hand, only half believe that customers expect their privacy to be respected. In our view this situation will change mainly because more and more business entities will be operating based on complex data processing methods and relevant conclusions from the data. Data is the currency of the digital world and the loss of data may turn out to be very painful for the business.

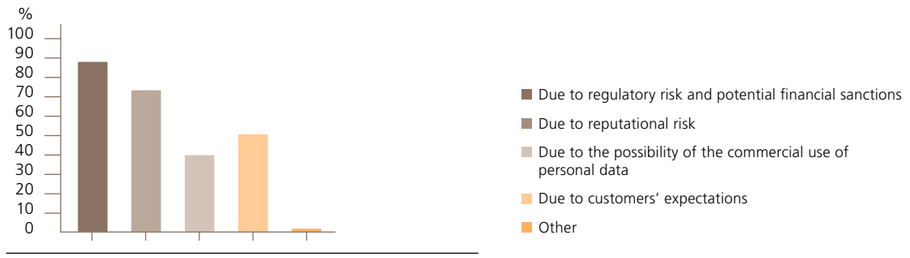
In your opinion, are business entities properly informed about the upcoming changes?



We will carry out educational and information activities to support the obliged entities in complying with the new principles of processing personal data specified in the EU regulation

dr Edyta Bielak-Jomaa, GIODO

In your opinion, why is it worth complying with the new EU personal data protection regulations?



Personal data protection 2.0

The new EU regulation amending the principles of personal data protection entered into force on 25 May 2016.

The new law is common and – as a rule – uniform for the entire European Union. For the Polish data protection system this means that this extensive regulation will replace the currently applicable Personal Data Protection Act, probably in its entirety.

Furthermore – and this is worth underlining – the EU regulation will apply not only to businesses from the European Union but also to those that have their registered office outside the EU but offer their goods or services to EU citizens or monitor their behaviour.

Advantages for consumers

The new regulations significantly strengthen the rights of natural persons being data subjects. They do not prohibit deriving benefits from processing customer data, however, they formulate specific rules of conduct and the resulting obligations, making the entire process of data processing transparent.

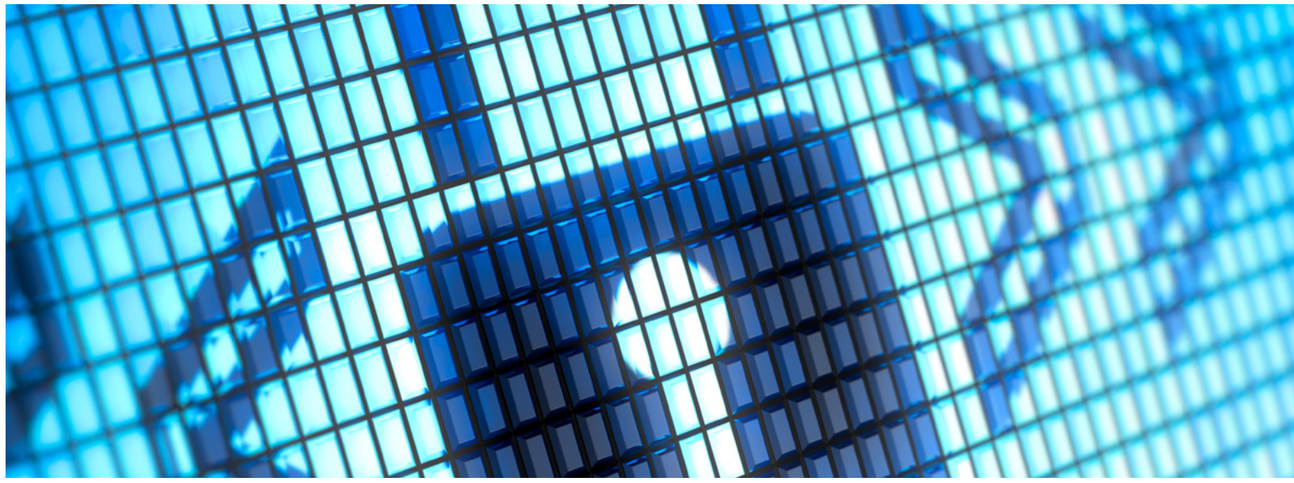
In practice this means that the times when the issue of personal data protection was not treated seriously by some entities will be long gone. What not so long ago was good practice will become an obligatory standard of operation for Polish business entities.

More obligations for companies

Placing the focus on the transparency of data processing and informing individuals on collecting and using their data will be a significant challenge for many companies. A business entity will have to ensure that all information and communications related to data processing are easily accessible, comprehensible and formulated in clear and simple language.

> The regulation will apply to all business entities in the European Union as well as to entities outside the EU which offer their goods or services to EU citizens or monitor their behaviour.

At the same time the scope of information provided to individuals by the personal data controller will be extended. Such scope will include e.g. information on profiling, the right to move data to another service provider, the right to withdraw the consent or information on the period of storing personal data.



Only secure subcontractors

As compared to the currently applicable Act, the new EU law requires much greater responsibility and awareness during the processing of personal data. The above concerns both data controllers and entities that process data on a fee or contract basis.

Data controllers will be able to entrust data processing only with entities that guarantee the proper implementation of the regulation and among other things, apply security measures adequate to the processing risk and regularly monitor the effectiveness of technical and organisational security resources.

ABI 2.0 i.e. Data Protection Officer

The new regulation significantly changes the role of the information security administrator. According to the regulation this role will be replaced by the data protection officer. One officer will be able to operate in more than one company only on the condition that it is easy for each company to contact the officer. This should improve the functioning of capital groups that coordinate activities aimed at data protection.

The catalogue of the officer's tasks has been unified in the entire European Union. The officer's duties will include monitoring compliance with the regulation by undertaking activities and training the employees of a given company as well as cooperating with the Inspector General for the Protection of Personal Data (GIODO). Penalties will be very severe – even EUR 20 million or 4% of the global annual turnover in the preceding financial year.

> Penalties will be very severe – even EUR 20 million or 4% of the global annual turnover in the preceding financial year.

Severe sanctions

The EU legislator provides two years for the Member States, the personal data protection authorities and business entities to fully comply with the new requirements. The regulation will be enforced starting from 25 May 2018.

In order to ensure that the regulation is observed, the EU legislator did not hesitate to implement severe sanctions. The new regulation allows for financial penalties in almost 30 cases, for example in the case of a failure to fulfil the obligations related to the terms and conditions of obtaining the consent for data processing or failure to fully inform the supervisory authority about a data leak.

The penalties may be very severe for business entities – even EUR 20 million or 4% of the global annual turnover in the preceding financial year (whichever is higher).

Consequences for the business

All business entities operating in Poland will have to conduct their activity in compliance with the new EU personal data protection law.

Below please find examples of challenges for businesses within the scope of personal data protection:

The principle of transparency

All the individuals whose data is processed by a company, for instance employees or customers, must be informed about what is happening to their data to a much greater extent than previously. Business entities will have to ensure that such information is transparent, reliable and clear.

A reliable choice of the data processor

Business entities will be responsible for assessing whether a given provider of data processing services has all the technical and organisational measures necessary for this purpose. Therefore, it may be advisable to already consider implementing a new procedure of selecting providers or adjusting the currently existing one to the more demanding legal environment.

Customer profiling

Changes in the scope of automated processing of personal data are the elements of the EU regulation that are key to business operations. The new law allows for profiling based on the automated processing of data only once the data subject's consent has been obtained, unless the profiling is necessary for the purpose of executing or performing an agreement. Under the regulation consumers must be informed about being subjected to profiling. Business entities will have to implement appropriate mechanisms to guarantee profiling-related rights to natural persons, in particular the right to object against a decision based on profiling.

Data security

The Regulation devotes much space to the issue of personal data security. Under the new provisions business entities are required to notify the GIODO and sometimes also data subjects (for instance customers) about all incidents of data breaches. All irregularities in this respect must be notified to the supervisory authority (GIODO) without undue delay, if possible – not later than within 72 hours. This relates not only to situations when data is, for instance, unlawfully published on the Internet, but also when a flash drive containing data is lost or data is deleted.

Data Protection Officer

Under the Regulation, it will be obligatory to appoint a data protection officer in the private sector in the following two cases: when the processing of data, due to its attributes, nature, purpose or scope, requires the regular and systematic monitoring of individuals on a large scale, and when special category data (sensitive data) or personal data concerning convictions is being processed on a large scale. In other cases, the appointment of a data protection officer will be voluntary.

Adapting to the new regulations

For many business entities it will be quite a challenge to adapt their operations to the new law in such a short period of time, i.e. by 25 May 2018.

It may turn out that ensuring technical, organisational and financial means necessary to operate in compliance with the new requirements is a long-term, tedious and – in most cases – expensive process.

Start now!

We recommend you start as soon as possible. Only the prompt and accurate identification of potential risks associated with data processing will allow you to react effectively. For this purpose, you must precisely analyse your business processes and compare them with the requirements of the new regulation.

Plan your work

It is necessary to prepare a detailed plan of action. On one hand, it should consider the importance of specific tasks to be carried out, on the other hand the organisational efforts involved in a given change.
The plan should identify specific individuals responsible for the implementation and specify the priorities, as well as the time that the company has at its disposal to implement the changes. You should also remember that some work will have to be performed within the company, while some will require cooperation with external partners – suppliers or customers.

Engage a team

We suggest creating a special working team, which will be responsible for the implementation of the changes and adapting the company to the new laws. The team should include a person responsible for the protection of personal data as well as representatives of the organisational units that will be influenced by the new regulation to the greatest extent. Such wide representation will ensure that the personal data protection is adapted in all the areas of the company's operations that are significant from the business perspective.

General Data Protection Regulation

1. Analysing whether it is obligatory to appoint a data protection officer for the whole group or its part in Poland or if it is just recommended due to the nature of the processed data.
2. Creating a diagram of data flow to the organisation, within the organisation and outside of the organisation; defining data sources, methods of collecting data; specifying entities with whom the data is shared; identifying risks related to the processes.
3. Analysing internal documentation related to the protection of personal data and creating – wherever possible – a standardised set of document forms for all the organisational units of the company and its branches.
4. Analysing software from the perspective of personal data security and requirements of the regulation, especially in the context of the Right to be Forgotten and Privacy by Design.
5. Analysing the risk of a Data Breach and the possibility of insuring oneself against the risk on the Polish/EU insurance market.
6. Developing the process of the Privacy Impact Assessment in relation to new projects involving personal data processing and implementing it in the company on a permanent basis.
7. Raising the awareness of the requirements that are imposed under the regulation on the employees, partners and clients of the organisation.
8. Verifying providers of services to the company from the perspective of their capability to effectively protect personal data in line with the provisions of the new regulation.
9. Renegotiating agreements on entrustment, which – according to the new law – must have quite extensive wording.
10. Fulfilling the information obligation resulting from the new regulation.

A reasonable approach

A conversation with the Inspector General for Personal Data Protection (GIODO), Edyta Bielak-Jomaa

foto: materiały GIODO

The regulation encourages business entities to create industry-related codes of good practice and join them. What is the GIODO's opinion on this issue? Does the GIODO think that such industry self-regulation may boost the level of data protection?

I believe that the so-called codes of good practice, which are a kind of a set of principles and standards of conduct relating to the processing of personal data are a solution that may help raise the level of personal data protection. The idea behind their development is not new, as it was laid down in Article 27 of Directive 95/46 / EC of the European Parliament and the GIODO has been initiating them and supporting their development for a long time.

The creation and approval of the codes of conduct (this is the name that has been given to them recently), has been regulated and formalised under the regulation much more precisely. The regulation provides for, inter alia, the approval and publication of the codes by the personal data protection authority, and it introduces a mechanism of monitoring compliance of provisions of such documents by entities accredited by the GIODO that have an appropriate level of expertise in the area to which the code applies. This, however, does not change the essence and purpose of their creation, which is, inter alia, to promote and unify the basic rules concerning personal data processing and to use them appropriately in practice.

It should be emphasised, however, that the drafting and use of the code as an instrument that makes it possible to prove that the data controller or the processor has duly implemented a guarantee concerning personal data protection is a rebuttable presumption, because neither the code's approval by the GIODO nor its monitoring by an accredited entity will exclude the powers of control of the personal data protection authority.

One of the obligations imposed on business entities under the Regulation will be the obligation to conduct the Privacy Impact Assessment, combined with the institution of prior consultation with the data protection authority. Does the GIODO foresee that the business entities operating in Poland will often use this form of dialogue with the regulator?

Considering how many requests for the interpretation of law in the context of solutions that are being applied or planned by the data controller the GIODO has received recently, I think that business entities will willingly take advantage of the possibility to consult the data protection authority, which is foreseen under the EU regulation. They will in fact treat it as a kind of a guarantee that the implemented mechanisms are compliant with the law and that in the event of the GIODO's inspection they will obtain a re-approval. It should be emphasised though that not everyone will be able to take advantage of such forms of cooperation with the GIODO. The provisions of the regulation limit the circle of eligible parties.

Firstly, when processing operations pose specific risks to the rights and freedoms of data subjects due to their nature, scope or purposes, the data controller or the data processor will be required to assess such risks, the impact of the project on privacy and the level of data protection.

Secondly, as stated in Article 36, if the assessment of the impact of the planned processing operations on data protection indicates that the processing would cause a high risk if the controller does not take any risk mitigating measures, the controller must consult the supervisory authority prior to commencing such processing. Moreover, under a Member State law the controllers may be obliged to consult the supervisory authority and obtain its prior consent for the processing of personal data for the purposes of tasks performed for the public interest, including processing related to social protection and public health. The regulation also stipulates that member states will consult the supervisory authority while preparing draft legislation adopted by the national parliament or a draft implementing act based on such legislation if it is related to data processing.

The Regulation provides for high financial penalties in the case of unlawful processing of personal data. Respondents believe that this is one of the decisive factors inducing them to process data lawfully. Does the GIODO believe that such high penalties will contribute to the raising of the level of data protection?

The Regulation introduces a completely new look at the position of the data controller and it transfers the burden of responsibility for the unlawful processing of personal data onto the data controller. And this is a rational approach, because the controller knows, or at least it should know, what measures to take in order to ensure the security of the data it processes.

This new approach brings about new sanctions. Their top level is EUR 20 million, and in the case of companies – 4% of the annual global turnover from the previous financial year. The penalties are assumed to be effective, proportionate and dissuasive. And I think they are.

In my opinion, knowing that you may pay a very high penalty for inappropriate data processing will motivate you to take greater care of the data.

Business entities have two years (just two years or as much as two years) to adapt their operations to the new provisions. Does the GIODO think that this period of time is sufficient? What, in the GIODO's opinion, should business entities do first to make good use of the adjustment period?

Although the Regulation will apply directly from 25 May 2018, it is worth taking a look at its provisions now and starting to prepare for it. The time left is not as long as it may seem. But where should you start? In my opinion, as a priority, it is necessary to assess your situation, review what data is processed and determine the purpose of processing it. The regulation introduces new data categories, such as biometric data, which have not been defined so far. You should also consider assessing the risk associated with a data breach. Only in this way can you introduce effective organisational and technical protection measures. The regulation increases the scope of the data controller's responsibility for the security of personal data, so it is in the company's interest to take care of it.

Is the GIODO planning to conduct any information campaigns, such as conferences or seminars on the new regulation or drafting any related information materials for business entities?

The GIODO began carrying out such educational activities from the moment work on the EU regulation commenced. Also, it was discussed during scientific conferences organised by the GIODO and other entities cooperating with the GIODO. Also, information about changes related to the EU regulation has been available on the GIODO's website. Thus, we will continue educational and information activities to help the obliged entities adapt to the new EU Regulation on personal data processing. I come from a scientific environment, so the issue of education is very important to me, and I will definitely continue the activities that I have been conducting in this area.

About CMS

CMS is an international law firm that provides comprehensive legal and tax advice to companies, financial institutions and administrative bodies. We are one of the largest and most experienced international law firms in Poland – we have operated on the Polish market for over 20 years.

The CMS office in Warsaw has 140 lawyers who advise clients from all key sectors of the economy. For more information see: **http://www.cms-cmck.com/Poland**

Prawnicy CMS mają bogate doświadczenie we wszelkich aspektach prawnych dotyczących ochrony danych osobowych. Obejmuje ono między innymi doradztwo strategiczne w kwestiach przetwarzania danych osobowych przez największych administratorów danych w Polsce i Unii Europejskiej, kompleksowe audyty zgodności przetwarzania danych osobowych z prawem, jak też doradztwo w zakresie procesów przekazywania danych poza Europejski Obszar Gospodarczy, w tym kwestii wiążących reguł korporacyjnych (BCR). Wielokrotnie reprezentowali klientów w postępowaniach prowadzonych przez GIODO.