Grant Thornton

An instinct for growth™

Purple Guide

Everything that an entrepreneur must know about GDPR

April/May 2018

Purple Guide
a source of information

We are pleased to present the next edition of the "Purple Guide", a series of studies where we discuss legal, accounting and HR issues important to entrepreneurs. This time, our study is devoted to issues related to the EU Regulation – GDPR.

We invite you to read it.

The EU Regulation, amending the provisions on the personal data protection will come into force from 25 May 2018.

The Regulation is applicable to all entrepreneurs, regardless of the scale and form of their business. With its entry into force, it will replace the Polish Act on the protection of personal data and will affect almost all areas of the company's activities. The changes introduced are primarily aimed at improving security and ensuring better protection of the personal data being processed.

Edward Nieboj
Managing Partner
Outsourcing Department
Grant Thornton

Who is covered by new GDPR rules?

The new rules apply whenever personal data are processed within the meaning of GDPR. It does not matter whether the processing is carried out by legal persons (e.g. capital companies, limited liability companies), natural persons (e.g. self-employed persons) or public administration bodies. It is also irrelevant whether the processor employs one person or thousands of people, whether it conducts commercial or production activities.

GDPR rules are always applicable when the data are processed by entities with an organisational unit located within the European Union, irrespective of whether the processing takes place within the EU. In addition, GDPR rules are applicable in a situation of processing data related to natural persons who are in the Union, by an entity with no organisational units within the EU, if the processing is related to the offering of goods or services to such persons or to the monitoring of their behaviour.

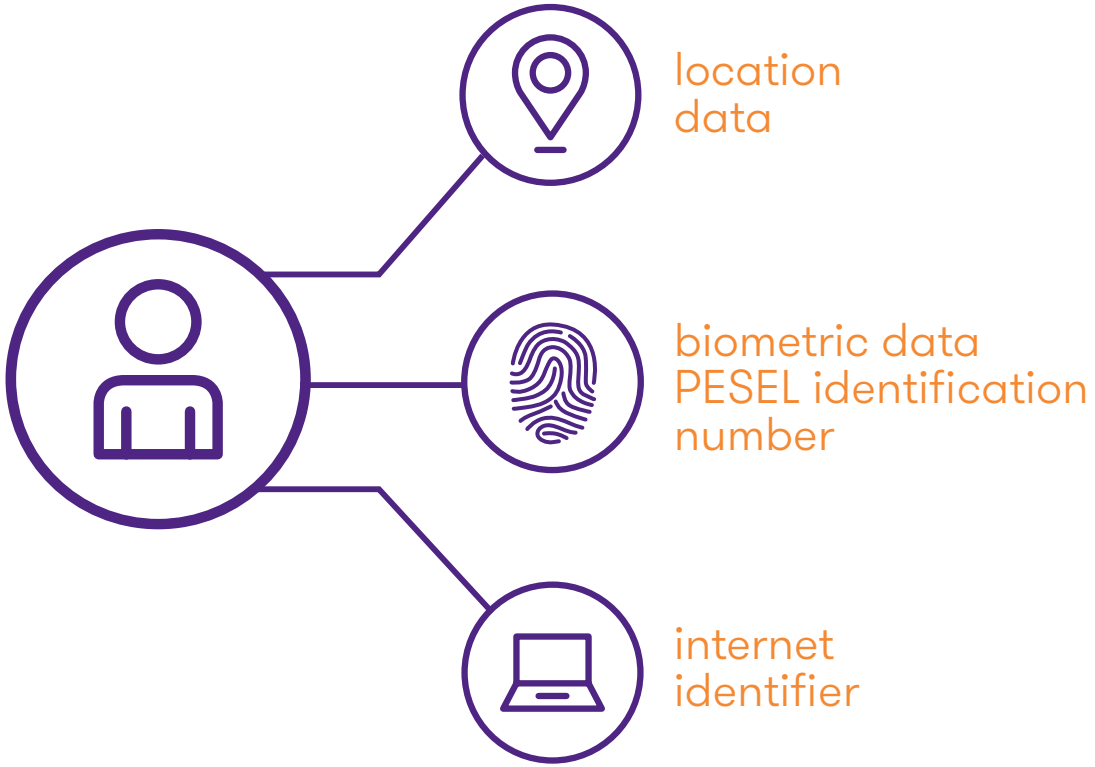
The subject related to the personal data protection concerns each of us. In practice, it is difficult to imagine that a business is run without processing personal data, such as staff data, contact details of customers and suppliers, personal data used for marketing or sales. In the case of some entities, the data are additionally processed on behalf of third parties. This concerns e.g. a marketing agency which prepares a conference and processes personal data provided by the entity commissioning organisation of that conference.

The protection of personal data applies to all of us.

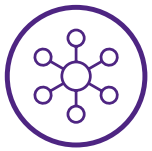
What are the personal data?

The personal data are a set of information about a natural person enabling his or her identification as a specific person, directly or indirectly.

The Regulation does not define a directory of data (e.g. name, surname, address) which will be considered as personal data. Such information as "Jan Kowalski" will not be the personal data, because many people in Poland have such a name and surname. On the other hand, a set of information, such as "Mr XXX, YYY street, ZZZ city, a tall dark-haired man" is so unique that it will allow identification of a specific person, so it will be treated as the personal data.



Who is a personal data controller?



natural or legal person, public authority, agency or other body

which, alone or jointly with others

determines the purposes and means of the processing of personal data

According to the definition contained in Article 4.7 of the GDPR, the controller can be a natural or legal person, public authority, agency or other body (the first component) which, alone or jointly with others (the second component), determines the purposes and means of the processing of personal data (the third component). The designation of the controller is a vital issue because it determines on whom the duties provided for in the GDPR are imposed and who is mainly responsible for the performance thereof. The determination of the Controller's role in specific cases of data processing is of special importance, especially in data processing performed within capital groups, in which there is a network of relations as well as actual and legal ties between companies in a group. In practice, most doubts arise over the second and third component, and therefore the first one will be omitted in this analysis.

To better understand the essence of the second component, the third one should be analysed first. The first criterion which allows for distinguishing the controller from other bodies taking part in processing is being actually capable of determining the purpose of data processing. While establishing who determines the purpose, fundamental questions should be asked as to why the processing is performed, who decides on that and what result of the processing is to be. Subsequently, one should determine if a decision-making body acts on its own behalf and for itself. On many occasions, in determining the role of the controller, the implied competence of bodies, arising out of their status in relation to data subjects, can be helpful, e.g. an employer in relation to its employees, or an association in relation to its members. The second criterion is the capability to determine the means of processing. To this end, a question should be asked as to who decides how the processing is performed. A means of processing should be understood as the technique and organisation of the processing. The technical aspect boils down to tools used for processing e.g. ICT systems, including the type of applications and software used (in this area, bodies processing data on behalf of controllers often hold a dominant position, e.g. entrepreneurs conducting outsourcing activity which impose a type of software, what, however, does not change their status as a processor). The organisational aspect, on the other hand, relates to how the processing is organised (how many persons take part in the processing, who are these persons, are these internal resources – employees, or external bodies to whom data are entrusted for processing), how long processing takes, what operations are performed on personal data. It should also be noted that it is on this ground where the discretionary power of the controller manifests itself over a means of processing, which the controller opting for the participation of a processor accepts or rejects the type of software and applications used by the latter

Speaking of the second component, the remarks made in the analysis of the third one should be taken into consideration, and it is the context in which the analysis of autonomy or non-autonomy should be made in the determination of the purpose and means of processing. Speaking of cooperation in determining the purpose, one should take into account a situation where two or more controllers jointly decide why and how the processing is to be performed. Emphases on joint actions do not have to be placed evenly, which means that the role of specific controllers in determining purposes and means may be different, but certainly each controller should contribute to some extent to the determination of a purpose. The given relation is well reflected by the example given in the Opinion 1/ 2010 on the terms "data controller" and "processor" given on 16 February 2010 - drawn up by the Working Party on the Protection of Data appointed under Article 29, in which a travel agency (controller I), carrier (controller II) and an owner of a hotel chain (controller III) jointly decide on the creation of an IT platform allowing for better management of a booking system. Taking collective actions by three independent controllers makes them joint controllers in relation to the specific processing purpose.

Who is the processor?

The definition of the processor is set out in Article 4.8 of GDPR.

For GDPR purposes, the"processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Thus the processor is the processing entity. Taking into account the whole personal data processing, processors are the main actors of processing, beside controllers.

Processors should be distinguished from persons involved in processing on behalf of personal data controllers, and remaining under direct supervision of controllers (e.g. employees, persons employed under civil law contracts). Such persons act within the organisational structure of controllers.

What distinguishes the processor from the controller is the absence of the decision-making powers as regards the purposes and means of processing, and also the organisational and legal independence distinguishing him from the processor. The controller decides about the purpose: e.g. data processing for the purpose of the employment relationship, and about the means of processing: selection of the operational program, selection of staff or a specific processor. The processor is independent of the controller in legal and organisational terms. Acting on behalf of the controller largely consists in acting on the basis of a documented controller's instructions regarding the designated purpose and method of processing.

The main processors include entrepreneurs providing outsourcing services in the field of HR, payroll, accounting, providing marketing services – marketing agencies, the services of destruction and archiving of documents, IT and hosting services.

What are the basic principles relating to the personal data processing?

7 main principles of personal data processing

The personal data processing principles fulfil two extremely important functions. First, as interpretative directives, they form the basis for interpreting GDPR rules. Secondly, they fulfil a normative function, i.e. they directly define the proper behaviour of the main actors in the personal data processing, i.e. the controller and the processor.

The first function may be illustrated by a situation in which the controller, in the absence of a clear instruction contained in a specific legal provision, wonders what form should be used for a given policy or procedure and whether the consent of the data subject may be given in verbal or written form. In such a case, it is justified to apply the accountability principle and to draw up a policy/procedure in a written form, in order to be able to demonstrate, e.g. to the supervisory body, that appropriate technical and organisational measures have been taken to ensure that the processing complies with GDPR. In the latter case, the controller should obtain written consent, or consent registration in the IT system ("clicking the consent box"), in order to demonstrate that such consent has been actually granted, the more so that GDPR rules as a whole may be interpreted as including a presumption of absence of consent.

As an example of the second application, one may mention the compliance principle or the data minimisation principle. The first principle requires the legal basis for the personal data processing to be specified in each case (e.g. by reference to the consent of the data subject or to compliance with a legal obligation). The second principle requires the personal data to be processed only to the extent that is necessary to achieve the purpose for which they have been collected and are to be processed, which means that personal data may not be collected "in advance".

The main principles are the following:

The principle of lawfulness - data may be processed only based on one of the legal prerequisites, e.g. the consent of a natural person (data subject), controller's obligation imposed by law.

The principle of purpose limitation – data may be processed only for the purpose for which they have been collected, if they have been collected to perform a contract, they may not be used for marketing purposes without prior notification to the person concerned (data subject) about the change of the purpose.

The principle of data minimisation – data may be processed only to the extent necessary in relation to the purposes of their processing, they may not be collected and processed "in advance".

The principle of accuracy – data must be substantively correct and for this purpose should be kept up to date, and data unsuitable for a particular purpose should be erased.

The principle of storage limitation – data may be stored only for the period needed to achieve the purpose and then they should be erased.

The principle of integrity and confidentiality – data must be adequately protected against accidental loss, damage, destruction (unauthorised processing), against access by unauthorised entities.

The principle of accountability – which applies only to personal data controllers, according to which the controller should be able to demonstrate compliance with GDPR rules. This means the necessity of adopting written procedures and documenting personal data processing, including the respect for rights of the persons concerned (data subjects).

What does the non-compliance with new GDPR rules mean for me, as an entrepreneur?

The consequences of non-compliance with GDPR rules for personal data controllers may be twofold.

First of all, they may involve institution of proceedings before the President of the Personal Data Protection Authority for the infringement of the personal data protection rules. The proceedings conducted by the President of the Personal Data Protection Authority may end with application of appropriate measures to force the infringer to remove GDPR infringements, such as, for example, an order to meet the demand of the complainant or financial sanctions.

financial sanctions

up to 20 million euros or including the demands of the person who has made the complaint

The latter may take the form of an administrative fine in the amount depending on the type of infringement. Controllers or processors infringing their obligation to implement appropriate organisational or technical measures and data security obligations are liable to a fine of up to EUR 10,000,000, and in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, however not less than the above fixed amount.

In the case of violation of the rules for processing personal data, of the legal prerequisites for the processing or of obligations to data subjects, the fine may amount up to 20,000,000 EUR, and in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, however not less than the above fixed amount.

Administrative fines shall be imposed by way of decision, in a single-instance procedure. The party will be entitled to appeal against the decision by lodging a complaint with the Voivodeship (Provincial) Administrative Court.

common court

Secondly, the described consequences may involve an action brought by the data subject before a common court. Proceedings before common courts will be conducted by civil divisions of district courts. To ensure maximum protection of data subjects' interests, the EU legislator provided for a joint and several liability of all entities involved in the processing. Passive joint and several liability means that the data subject may bring an action, at his/her own discretion, against one, two or all entities involved in the processing, and if the data subject's claim is satisfied by one of them, other entities shall be released from liability, however, the entity that has satisfied the claim may subsequently institute recourse proceedings against other entities.

What obligations are imposed on me, as an entrepreneur, in connection with new GDPR rules?

The main obligations of the entrepreneur, as the personal data controller, include implementation of GDPR rules in his/her company. To do this correctly, first the controller must make an inventory of the data processing operations in the organisation, including the personal data protection documentation and procedures.

Next, the level of risk associated with the personal data processing must be determined.

Afterwards, it is necessary to determine the scope of necessary changes in the documentation, or to take a decision on developing new documentation, depending on the level of risk associated with the data being processed. Risk assessment will allow controllers to properly determine the obligations to be met to ensure that data processing under their responsibility is performed in accordance with GDPR.

The main obligations of the personal data controllers include:

1. verification of information clauses and data subjects' consents in terms of their compliance with GDPR
2. assessment of risk to the rights and freedoms of data subjects and determining on this basis the most important controllers' obligations, such as creating and implementing a record of processing activities or designating a personal data protection officer
3. personal data protection impact assessment
4. creating and implementing a procedure for responding to personal data breach incidents
5. creating additional documentation or implementing additional security measures, e.g. procedures for determining/confirming the identity of persons applying for access to data
6. amending/signing contracts for entrusting personal data processing
7. introducing the principles of privacy by design and privacy by default to personal data processing

What should I do in a situation of personal data breach?

reporting to the administrator of personal data

or

reporting to the supervisory authority within 72 hours of finding the violation

Before answering this question we should define "personal data breach". Pursuant to Article 4.12 of GDPR, "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The personal data controller should notify such data breach to the supervisory authority not later than 72 hours after having become aware of it.

For example, an obligation to notify the breach will arise when one of the employees loses a portable personal data disk or a HR department employee leaves contracts of employment of other employees on the desk after working hours, in the presence of the cleaning service. Such an obligation will not arise if the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. For example, in the discussed case of the employment contracts left, if on the day of the incident there were no people in the employee's room from the moment of leaving these contracts until they were properly secured, because the room had been secured against access by other people.

However, if the personal data breach involves high risk to the rights and freedoms of the natural persons concerned, the personal data controller will be obliged to notify such person about the breach. Such incident may for example involve unauthorised public disclosure of personal data regarding the financial situation of a specific natural person, which poses a direct and high threat to his/her property, e.g. in the form of the threat of theft or fraud to his/her detriment.

The personal data controller's obligation to inform natural persons about the breaches is linked to the obligation to document any such breaches. Such documentation is to enable the supervisory authority to verify compliance with GDPR rules. However, if the personal data breach occurs in the scope of activities of the processor, the processor will be obliged to notify the personal data controller of this fact.

Does a large company have more obligations related to GDPR than the small one?

The new rules do not provide for a set of standard procedures, operations or mechanisms securing personal data. Their idea is to allow for adaptation of procedures, tools, technical and organisational solutions to the scope of data being processed, to objectives and risks related to the personal data breach. The solutions should be also developed with due regard to data processing frequency or context. An organisation that processes data on a smaller scale, processes less sensitive data or uses simple IT technologies, is able to meet GDPR requirements in a cheaper and faster way than entities with a complex organisational or operational structure.

On the other hand, such flexibility and freedom in adapting personal data protection tools is a challenge, because to effectively meet GDPR requirements, it is necessary to think through and adapt the solutions to the type of business. The system need not be complicated, it has to be adequate and effective. An approach that involves downloading a set of standard procedures from the Internet is out of the question.

In order to be able to effectively meet the obligations arising from the GDPR, we need to rethink and adapt the solutions to the type of business.

What are the risks for me, as an entrepreneur, associated with the implementation of new GDPR rules?

Most of us have certainly heard about the penalties introduced by the new rules. It is true that the change in this regard is revolutionary compared to the current rules. The maximum penalties amount to up to EUR 20 million or up to 4% of the total worldwide (!) annual turnover, whichever is higher. Additionally, the Regulation allows individuals to pursue claims in the event of the infringement of the personal data protection rules.

It should be, however, emphasised that effects of bad PR, loss of reputation resulting from data leakage may be much more dangerous for entrepreneurs. We also observe one more trend among large companies and corporations: their large awareness of the need to protect personal data. For example, they make the cooperation with a supplier subject to his meeting the requirements in the area of personal data protection.

It is worth mentioning that each of us transfers his/her personal data to various entities and we would certainly wish them to be protected and used only for the purpose for which they have been collected. For this reason we also should be able to guarantee in our organisations the same solutions as those we expect from others.

loss of reputation

in the event of a data leak

financial penalties

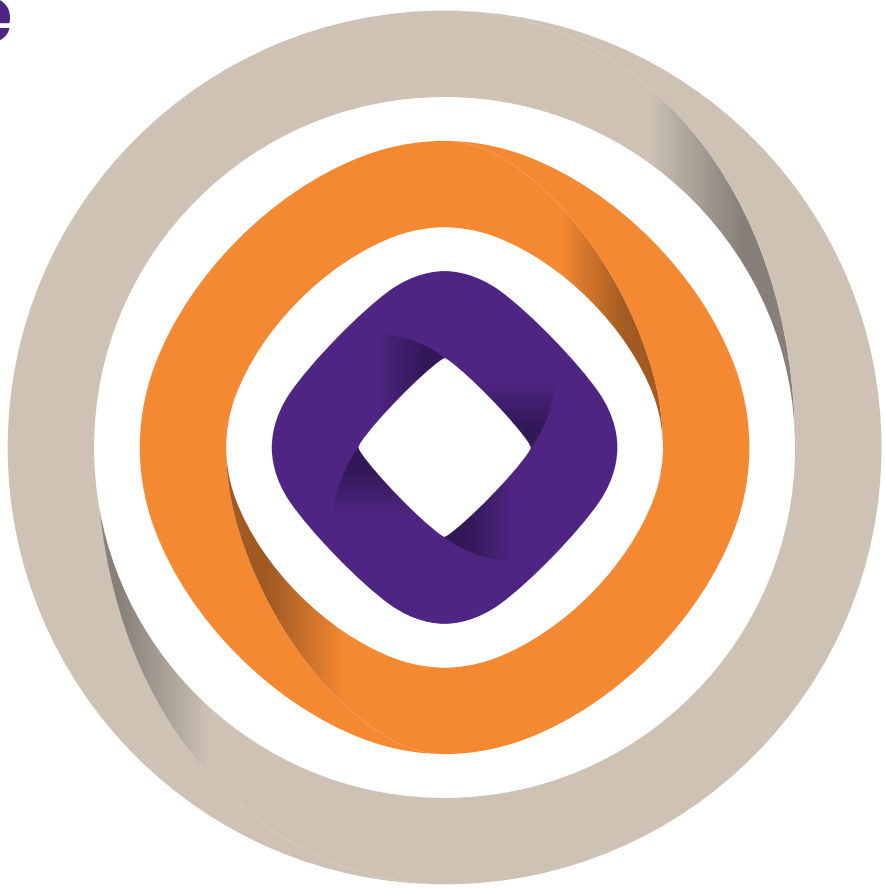
up to EUR 20 million or up to 4% of the total worldwide annual turnover

Is it a long and costly process to prepare for GDPR?

It depends on several factors. We must remember that the data protection system must be adapted to a company concerned. Te process can be, certainly, long and costly for large, international organisations.

However, for smaller organisations, in many cases it will be quite the opposite. Many organisations have already implemented mechanisms ensuring a considerable level of personal data protection, e.g. an obligation of periodic change of password to the computer, access cards to office premises, lockers for documents, data backup procedures, anti-virus programs, etc. Thus, it may prove that the effort must be mainly directed to document the entire process, to provide for appropriate clauses of consents, impose information obligations, train employees or change certain habits (e.g. introduce clean desk policy).

Will the use of outsourcing services in HR/payroll/ accounting issues be safe for the company after 25 May 2018?



Yes, such solution is completely safe and compliant with new GDPR rules.

One should, of course, cooperate with a reliable partner who is able to ensure the security of personal data. It is absolutely necessary remember about signing a contract for entrusting personal data.

One should remember that the contract for entrusting personal data should be signed with each entity to whom the data have been entrusted. This applies, in particular, to companies which store or destroy documents, companies which provide IT solutions based on the cloud, etc.

Can Grant Thornton support me in GDPR implementation and how such support would look like?

Our organisation can offer support in implementing solutions required by GDPR. We can help you both at the stage of identification of measures to be undertaken, the procedures to be implemented, but we can also help you in their implementation.

We propose two cooperation models:

Outsourcing of the GDPR area

which will ensure that the solutions and procedures in this area will be kept up to date, and it will remove the need for the organisation to maintain knowledge and expertise.

GDPR help desk

i.e. a possibility of quick contact with people who are experts in this area. In this case, our job will be to provide support, e.g. by means of answering any questions that can arise or reacting to the need to modify existing documentation. documentation.

sources:
1. Regulation of the European Parliament and of the Council (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),
2. E. Bielak - Jomaa, D. Lubasz, red. Naukowa „RODO Ogólne Rozporządzenie o Ochronie Danych" (General Data Protection Regulation), Commentary, Wolters Kluwer, Warsaw 2018,
3. B. Fischer, M. Sakowska – Baryła, „Realizacja praw osób, których dane dotyczą na podstawie RODO" (Implementation of rights of data subjects on the basis of GDPR), PRESSCOM sp. z o.o., Wrocław 2017 r.,
4. Polish draft Act on the protection of personal data, available on the website https://www.gov.pl/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych.
5 Opinion 1/ 2010 on the terms "data controller" and "processor" given on 16 February 2010, available on the website https://giodo.gov.pl/261

Edward Nieboj
Managing Partner
Outsourcing Department
Grant Thornton
T +48 693 333 386
E Edward.Nieboj@pl.gt.com

Tomasz Dziedzic
Legal Adviser
Expert cooperating with
Grant Thornton
T +48 691 998 701
E Tomasz.Dziedzic@pl.gt.com

For over 20 years, we have been dealing at Grant Thornton with processing personal data of our clients as part of our outsourcing services. In our everyday work we do care about the personal data security, while adapting to the upcoming changes. We hope that the present material has shown that we are ready to support you also in issues related to GDPR.

Should you have any questions or concerns, please contact us. Our team of experts is at your disposal!

Grant Thornton
An instinct for growth™

www.GrantThornton.pl