THE MAIN NOVELTIES AND IMPLICATIONS OF THE NEW GENERAL DATA PROTECTION REGULATION

Lecturer **Simona CHIRICA**[1]

Abstract

*Regulation (EU) 2016/679 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) - **GDPR** will become applicable beginning with 25.05.2018. As a general characteristic, the regulations adopted at EU level, have direct applicability in all EU member states, and they are automatically integrated in the national legislation beginning with entry into force. Therefore, as of 25.05.2018, the GDPR provisions will be applicable and mandatory for all natural and legal persons that process personal data, including in Romania. Based on the above, GDPR brings a series of changes affecting all the involved parties (data subjects, data controllers, supervisory authorities). This article aims to present an analysis of the main novelties brought by the new regulation, and to present a comparison with the current regulation together with the practical implications of these changes in relation to the data subjects, data controllers, and supervisory authorities.*

Keywords: *Regulation (EU) 2016/679, General Data Protection, personal data security, supervisory authorities.*

JEL Classification: K23, K24, K33.

1. Introduction

Nowadays, personal data processing aspects are regulated at national level in Romania by Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Law 677"). This law represents the transposition of Directive 95/46/CE of the European Parliament and Council from 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

In 2016, the European Parliament and the Council adopted the GDPR, pursuing mainly, on the one side, to grant more responsibility to the personal data controllers, and on the other side, to strengthen the rights of the data subjects, but also to introduce new rights for the data subjects[2].

Thus, GDPR brings the following novelties:

2. From the perspective of the data subjects

2.1. The consent and information of the data subject

In terms of information of the data subject, Law 677 stipulates the right of the data subject to be informed of the processing of his/her personal data and the data controller has the obligation to provide him/her, the following information, except where he/she already has it:[3]

a) The identity of the data controller and his/her/its representative, if any;
b) The purpose of the data processing;
c) Additional information, such as: the recipients or the categories of recipients of the data; whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; the existence of the rights provided by law for the data sub-

[1] Simona Chirica – Department of Law, Bucharest University of Economic Studies, Romania, s.chirica@schoenherr.eu

[2] New Regulation (EU) 2016/679 applicable from 25th May 2018 - Novelties (Flyer) published on ANSPDCP website http://dataprotection.ro/?page= Regulamentul_nr_679_2016 (consulted on 1.10.2017).

[3] Art. 12 of Law 677.

ject, particularly the right of access, the right of intervention and opposition and also the conditions under which they can be exercised;

d) Any other information imposed by the supervisory authorities, taking into consideration the specificity of the processing.

GDPR extends the range of aspects that are subjects to the information obligation; therefore, beside the above mentioned information, according to art. 13 from GDPR, the data controller has the obligation to provide the data subject, the following information, except where he/she already has it:

a) The identity and the contact details of the data controller and, depending on the situation, the contact details of his/her/its representative;
b) The contact details of the data protection officer in charge with the data protection, depending on the situation;
c) The purpose of the personal data processing and also the legal basis of the processing;
d) The legitimate interests pursued by the controller or by a third party, if the data processing is based on such interests;
e) The recipients or the categories of recipients of the personal data;
f) If applicable, the intention of the controller to transfer the personal data to a third country or international organization and a reference to the appropriate guarantees.

Moreover, in order to ensure a fair and transparent process, the data controller will provide the data subject with the following information related to processing:[4]

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
c) The existence of the right to withdraw the consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
d) The right to lodge a complaint with the supervisory authority;
e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;
f) The existence of an automated decision-making process, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

If the personal data were not obtained directly from the data subject, the data controller will inform him/her about the above mentioned aspects, including also the source from which the personal data originate and whether the data originate from public sources.[5]

The consent of the data subject. The complete provision of all information is important, particularly in the context of obtaining the data subject's consent for the processing of his/hers personal data. According to GDPR[6] the consent of the data subject should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of his/her personal data, such as a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his/her personal data. Abstention, pre-ticked boxes, or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes.

[4] Art. 13, para. 2 GDPR.
[5] Art. 14, para. 2 lit. f) GDPR.
[6] Preamble 32 of GDPR.

When the processing has multiple purposes, consent should be given for all of the envisaged purposes. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise, and not unnecessarily disruptive to the use of the service for which it is provided.

In the cases where the processing is based on consent, the data controller should be able to demonstrate that the data subject has given his/her consent for the processing of the personal data.[7] The request for the consent should be presented in an intelligible and easily accessible form, using clear and plain language and if the data subject's consent is given in the context of a written document that also concerns other matters, the request for consent shall be presented in a manner, which is clearly distinguishable from the other matters.[8] Moreover, the consent won't be freely given if the data subject didn't have a real option to agree to his/her personal data processing; for example in the situation where the provision of a service, is conditioned on the consent to the processing of personal data that are not necessary for the performance of that contract.[9]

Furthermore, in this context it should be also taken into account the situation where the data subject is **underage**. In such situations the underage subject can validly give his/her consent only if he/she is at least 16 years old. Otherwise, the holder of parental responsibility will be able, depending on the situation, to give the consent or to authorise the consent. In this way, GDPR forces the data controllers to make all reasonable efforts in order to check if in this kind of situations the holder of parental responsibility has given or authorised the consent, according to the available techniques.[10] At the same time, GDPR offers the possibility for the Member States to decide within their national legislation a different, lower age, needed for validly expressing consent, but this age should not be below 13 years.[11] In Romania, such regulation hasn't been adopted yet. It remains to be determined, if the Romanian legislature will consider such regulation necessary, taking into consideration that the national legislation stipulates a limited legal competence starting with 14 years.

Another important aspect refers to the fact that the data subject has the right to withdraw his/her consent anytime and this withdrawal must be as simple as giving the consent. The consent withdrawal creates the mandatory obligation for the data controller to delete that person's data.[12]

2.2. The right to data portability

A new right introduced by GDPR refers to the personal data portability. The data portability complements the data subject's right of access, stated also in the actual regulation. Unlike the right of access, the data portability right offers for the data subject an easy way to handle and reuse the personal data transmitted to a business operator.[13] In this way[14], the data subject has the right to receive his/her personal data, which he/she provided to the data controller, in a structured and frequently used format, which can be read automatically, having the right to transmit the data to another data controller, without impediments from the data controller to whom the data were initially provided, in the following cases:

a) The processing is based on the data subject's consent, or on a contract between the data subject and the data controller; and
b) The processing is carried out through automated means.

At the same time, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.[15] The technical possibilities to

[7] Art. 7, para. 1 GDPR.
[8] Art. 7, para. 2 GDPR.
[9] Art. 8, para. 2 GDPR.
[10] Art. 8, para. 2 GDPR.
[11] Art. 8 GDPR.
[12] Art. 7, para. 3 and art. 17, para. 1 letter b) GDPR.
[13] "Article 29" Data Protection Working Party -"Guidelines on the right to data portability", revised and adopted on 05.04.2017, p.5.
[14] Art. 20, para.1 GDPR.
[15] Art. 20, para. 2 GDPR.

transmit the data from one data controller to another, under the control of the data subject, are evaluated on a case-by-case basis. It is expected that the data controllers transmit the personal data in an interoperable format, but at the same time the other data controllers don't have the obligation to assure the technical support for one specific format. Therefore, the direct transmission of data from one data controller to another could appear when the communication between two systems is possible, in a secured way and if the data receiving system has the technical capacity to receive the transmitted data. In the cases where the technical impediments don't allow the direct transmission of data, the data controller has to explain these impediments to the data subjects.[16]

Regarding the **data that are subject to the right to data portability**, such data is limited to the personal data that were provided to the data controller by the data subject. however, it is claimed[17] that, in order to offer a complete value to this new right, the portability should include, beside the data provided by the data subject, also the personal data that can be observed from the user's activities (for example, the history of searching and website using, activity journals). Moreover, the portable data can also refer to other data subjects. The data subject can initiate the transfer of a third party's data, if (i) these data remain under the data subject responsibility and (ii) the data are transferred to another data controller for the same processing purpose.[18]

The right to data portability has as main objective, the empowerment of the data subject and it intends to grant the data subject a better control over his/her personal data, facilitating the data subject with the possibility to easily move, copy and transmit his/her own data from one IT environment to another.[19] As a consequence, data controllers are encouraged to ensure and develop the necessary means to accomplish all the data portability requests from data subjects, for example through download instruments and application programming interface.[20]

However, the right to data portability has also exceptions. The right to data portability cannot prejudice the right to erasure or limit the other data subject's rights and freedoms. The right to data portability should therefore not apply where the processing of the personal data is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.[21]

3. From the perspective of the data controllers

3.1. The data protection officer (DPO)

A. The cases where a DPO is mandatory. GDPR introduces through art. 37-39 the data protection officer's position (DPO). Thus, data controllers and processors will be forced to name a DPO in the following situations:

a) If the processing is carried out by a public authority or public body, excepting the courts which are acting in their judicial capacity;
b) If the **core activities** of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects **on a large scale; or**
c) The **core activities** of the controller or the processor consist of processing **on a large scale** of **special categories of data**[22] **and personal data relating to criminal convictions and offences**[23]**.**

[16] "Article 29" Data Protection Working Party -"Guidelines on the right to data portability", revised and adopted on 05.04.2017, p.17.
[17] *Ibidem*, p.10.
[18] *Ibidem*, p.10 and 12.
[19] *Ibidem*, p.10 and 4.
[20] *Ibidem*, p.10 and 3.
[21] Art. 20, para. 3 and 4 GDPR.
[22] See art. 9 GDPR.
[23] See art. 10 GDPR.

GDPR grants the Member States the possibility to include in their national law also other cases where the designation of a DPO is needed. In the other situations, where the designation of a DPO is not mandatory, the data controllers or the processors can still consider that a DPO is useful and they can name a DPO voluntarily. In this situation the same requirements for designation, position and tasks are applicable as if the designation of DPO was mandatory.[24]

Regarding the notion of "main activity"[25], this includes the key operations done by operators or processors in order to achieve their goals. It refers to activities in which the data processing represents an indissoluble and inherent part. For example, in a hospital the processing of data regarding the health condition of the patients can be considered as one of the main activities, so hospitals will have to name a DPO. On the other hand, the activities needed for the worker's payment of wages are rather auxiliary activities than main activities.

Regarding the notion of "on a large scale", GDPR doesn't offer a definition of this concept. Some criteria are recommended in order to decide if a processing is done on a large scale; through this criteria we can enumerate:[26]

- The number of data subjects;
- The volume of processed data and/or the range of different processed elements;
- The duration of the processing activity;
- The geographic area of the processing activity.

Regarding, the "systematic and periodic monitoring", neither this notion is defined by GDPR, but it was concluded that it includes all the forms of tracking and profiling on internet, including for the purpose of behavioural advertising (for example, operating a telecommunication network, tracking a location through mobile apps, loyalty programs, wellness, fitness and health data monitoring through portable devices, etc.).[27]

B. The position of DPO. According to GDPR[28], the DPO has the following functions within the activities of the data controller or processor:

a) He/she is involved, properly and in a timely manner, in all issues which relate to the protection of personal data;
b) all the necessary resources will be provided for him/her to carry out those tasks and access to personal data and processing operations, and to maintain his/her expert knowledge.
c) He/she does not receive any instructions regarding the exercise of his/her tasks. He/she shall not be dismissed or penalised for performing his/her tasks.
d) He/she shall directly report to the highest management level of the controller or the processor. However, the DPO will not be personally responsible for the existence of non-compliance cases regarding the data processing requirements. The data controller or processor will still be the ones obligated to ensure appropriate technical and organisational measures and to demonstrate that the processing is carried out in accordance with the GDPR;[29]
e) He/she will be the contact person for the data subjects, regarding all issues related to the processing of their personal data and to the exercise of their rights under the GDPR;
f) He/she shall be bound by secrecy or confidentiality concerning the performance of his/her tasks;
g) He/she may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests. In this context, a DPO can't

[24] "Article 29" Data Protection Working Party - "Guidelines on the data protection officer (DPO)", revised and adopted at 05.04.2017, p. 20.
[25] I*bidem*, p.20.
[26] *Ibidem*, p.21.
[27] *Ibidem*, p.21.
[28] Art. 38 GDPR.
[29] "Article 29" Data Protection Working Party - "Guidelines on the data protection officer (DPO)", revised and adopted at 05.04.2017, p. 25.

hold a position within the organization, which could grant him/her the possibility to set goals and means of data processing;[30]

h) A group of companies can name a sole DPO, under the condition that he/she will be easy to reach from every company and can efficiently fulfil the tasks for every company. In order to make the DPO reachable it is recommended that he/she be located in EU, even if the data controller or processor is outside the UE.[31]

i) The DPO can be an employee of the data controller or processor or can be employed under a service agreement (as an extern). This service agreement can be concluded with a natural person or an organization; in the latter case it is necessary that every member of the organization fulfils all the requirements imposed by GDPR.[32]

C. The tasks of the DPO. The DPO will be named based on his/her professional qualities and specialty knowledge about the law and practices in the data protection field. The required level of experience will be determined according to the processing operations and protection needed (for example, if the processing operation is complex or it involves special categories of personal data, the DPO will need a higher level of experience). Thus, among the relevant skills and experience are included:

- Experience regarding the legislation and national/European data protection practices;
- Understanding of the performed processing operations;
- Understanding of information technologies and data security;
- Knowledge of the business sector and the organization;
- Ability to promote data protection within the organization.[33]

Therefore, considering these skills and experience, the DPO will have at least the following tasks:[34]

a) to inform and advise the controller or the processor and the employees who carry out data processing of their obligations;

b) to monitor the compliance with GDPR, with other EU or national data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c) to provide advice where requested as regards the data protection impact assessment and monitor its performance;

d) to cooperate with the supervisory authority;

e) to act as the contact point for the supervisory authority on issues relating to the processing.

3.2. The data protection impact assessment (DPIA)

GDPR introduces the concept of impact assessment on data protection. This kind of assessment represents a process, which describes the processing and analyses the necessity and proportionality of the processing, in order to diminish risks for the rights and freedoms of data subjects resulting from the processing of their personal data.[35]

According to art. 35 the data protection impact assessment will be carried out when the processing is likely to generate a high risk for the rights and freedoms of natural persons. The risk level is appreciated in accordance with the nature, field of application, context and processing purposes.

[30] *Ibidem*, p.24.
[31] *Ibidem*, p.22.
[32] *Ibidem*, p.23.
[33] *Ibidem*, p.23.
[34] Art. 39, para. 1 GDPR.
[35] "Article 29" Data Protection Working Party -„Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, adopted on 04.04.2017, p.4.

GDPR provides also a series of examples, in which the data protection impact assessment is mandatory, as follows:[36]

a) for systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) for processing on a large scale of special categories of data or of personal data relating to criminal convictions and offences; or
c) for a systematic monitoring of a publicly accessible area on a large scale.

Moreover, GDPR[37] stipulates the obligation of the national supervisory authorities to draw up a list of the processing operations which are subject to the requirement for a data protection impact assessment.

Also, when deciding which types of processing need a data protection impact assessment, the following **criteria** must be taken into consideration:[38]

- Evaluation or scoring: including profiling and predicting aspects concerning the data subject's performance at work, economic situation, health, preferences or personal interests, reliability or behaviour, location or movements (for example, if a company offers genetic tests directly for the consumer, having the purpose to evaluate and predict disease risks);
- Automated decision making: with legal effects or which similarly and significantly affects the data subject (for example, the automatic deny of an online credit request or online recruiting, without human intervention);
- Systematic monitoring: includes as a criteria, also systematic monitoring of areas that are accessible for the public;[39]
- Sensitive data: includes special categories of data and data relating to criminal convictions and offences (for example, when a hospital keeps the medical records of patients or when a private investigator keeps the suspect's data);
- Processing on a large scale: GDPR does not define the notion of "large scale". However, there are some criteria which are recommended, in order to decide if a processing is carried out on a large scale; among this criteria are included:
  - The number of data subjects;
  - The volume of data processing and/or the variety of different processed elements;
  - The duration of data processing activity;
  - The geographic area of the processing activity.
- Data sets which have been matched or combined: for example, when such data come from two or more processing operations carried out with different purposes or by different data controllers;
- Data on different vulnerable data subjects: a processing of this kind of data can require a data protection impact assessment considering the disproportion of power between the data subject and data controller. This category may include the employees in relation to their personal data processed by the employer, children, but also mentally ill persons, old people or patients.
- Innovative use or application of technological or organisational solutions: for example, the combined use of fingerprints and facial recognition in order to grant access. Regard-

[36] Art. 35, para. 3 GDPR.
[37] Art. 35, para. 4 GDPR.
[38] "Article 29" Data Protection Working Party -,,Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, adopted on 04.04.2017, p.7-8.
[39] This kind of monitoring represents a criterion because the data could be collected in circumstances where the data subject doesn't certainly know who the data controller is and how he is going to use the data. Also, for data subjects it would be impossible to avoid the data processing in this kind of locations, frequented by public.

ing this matter, GDPR stipulates that using new technologies may trigger the need to have a data protection impact assessment, because using this kind of technology may also include new forms of collecting and use of data, with a possibility to generate a high risk for the rights and freedoms of the data subjects.

- The transfer of data outside UE: it shall be taken account, amongst others, the destination states, the possibility of a subsequent transfer and the probability of transfers based on derogations for specific situations.[40]

The more criteria are met in a processing operation, the more obvious it will be that the data protection impact assessment is necessary.[41] This impact assessment shall be performed before starting the processing and an unique/sole assessment can approach a set of similar processing operations, which presents similar high risks.[42]

If some modifications appear amongst the risks of processing, then an analysis will be conducted, in order to evaluate if the processing is performed according to data protection impact assessment.[43] Thus, the data controller will assure that the assessment is updated over the lifetime of the project for which the personal data processing is carried out. Therefore, the data protection impact assessment represents a continuous process and not a single act.[44]

The persons involved in the data protection impact assessment. The data controller is responsible with the data protection impact assessment. The assessment can also be performed by another person within the data controller or by an extern, but under the responsibility of the data controller.[45] If a DPO was appointed, he/she should be consulted and his/her point of view shall be a documented in the assessment process.[46]

If the processing is performed through a processor, he will assist the data controller in the impact assessment and will provide all the needed information. The role and the responsibilities of the processor will be set contractually.[47]

---

[40] Derogations for specific situations are stipulated in GDPR under art.49 (1), which states as follows:
(1) "In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:
(a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
(b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
(d) the transfer is necessary for important reasons of public interest;
(e) the transfer is necessary for the establishment, exercise or defence of legal claims;
(f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
(g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.
Where a transfer could not be based on a provision in Article 45 or 46, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued."

[41] "Article 29" Data Protection Working Party -,,Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, adopted on 04.04.2017, p.9.

[42] Art. 35 para. 1 GDPR.

[43] Art. 35 para .11 GDPR.

[44] "Article 29" Data Protection Working Party -,,Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, adopted on 04.04.2017, p.13.

[45] *Ibidem*, p.13.

[46] Art. 35 para. 2 GDPR.

[47] "Article 29" Data Protection Working Party -,,Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, adopted on 04.04.2017, p.13 and 14.

Moreover, according to GDPR[48], where appropriate, the controller shall seek the views of the data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations. This kind of views can be obtained through diverse ways, (like: intern studies, formal questions addressed to employees, a questionnaire etc.) and the data controller should document the data subject's points of view and also justify why he didn't consider a point of view necessary.[49]

Furthermore, the data protection impact assessment may involve the contribution of independent experts, like lawyers, technicians, sociologists, IT specialists.[50]

The content of data protection impact assessment. According to GDPR[51] the assessment shall contain at least:

a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
c) an assessment of the risks to the rights and freedoms of data subjects; and
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with GDPR, taking into account the rights and legitimate interests of data subjects and other persons concerned.

Compliance with approved codes of conduct shall be taken into due account in assessing the impact of the processing operations performed by controllers or processors.[52]

Prior consultation of Supervisory Authority. GDPR[53] imposes for the data controller the obligation to consult the supervisory authority in the situation where, after the data protection impact assessment, the residual risks remain high and the controller cannot find sufficient measures to address these risks.[54]

Where the supervisory authority is of the opinion that the intended processing would infringe the GDPR, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor. This period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained the information it has requested for the purposes of the consultation.[55]

Moreover, GDPR[56] grants the Member State's the possibility to stipulate in their national law other situations when controllers have to consult, and obtain prior authorisation from the supervisory authority in relation to a processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

---

[48] Art. 35, para. 9 GDPR.
[49] "Article 29" Data Protection Working Party -„Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, adopted on 04.04.2017, p.13.
[50] Ibidem, p.14.
[51] Art. 35 para. 7 GDPR.
[52] Art. 35 para. 8 GDPR.
[53] Art. 36 para. 1 GDPR.
[54] "Article 29" Data Protection Working Party -„Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purpose of Regulation 2016/679, adopted on 04.04.2017, p.18.
[55] Art. 36. para. 2 GDPR.
[56] Art. 36. para. 5 GDPR.

3.3. Organising the intern procedures (''Privacy by design'' and ''Privacy by default'')

In order to permanently ensure a high level of protection on personal data, the data controller should elaborate internal procedures that guarantee data protection compliance in every moment, taking into consideration all the events that may appear during the data processing.[57]

At this time, in order to guarantee the data protection and the security of the processing at the national level, Order of Ombudsman no. 52/2002 on approval of the minimal security requirements for personal data processing (**''Order 52/2002''**) is applicable. This order establishes the minimal technical and organisational measures which should be taken by every data controller or processor, in order to assure an adequate protection of personal data.

Once the new regulation becomes applicable, GDPR stipulates under art.25 para. 1 that these technical and organisational measures will be evaluated depending on the state of the technology, the cost of implementation and the nature, scope, context and purposes of processing and also depending on the risks for the rights and freedoms of natural persons posed by the processing. So, measures like pseudonymisation can be taken into consideration, or other measures that are able to effectively implement the data protection principles.

In this context, GDPR introduces two new concepts referring to personal data processing, one is the concept of *''privacy by design''* and the other is *''privacy by default''*. Thus, the controller shall implement suitable technical and organisational measures, **both at the moment of deciding the means of processing and also at the moment of processing** ("privacy by design"). Also, the controller shall assure that only personal data which are necessary for each specific purpose of processing are **implicitly** processed, by reference to the volume of the collected data, the level of processing, storage period and their accessibility ("privacy by default"). In particular, the conducted measures should ensure by default that personal data cannot be accessed by an unlimited number of persons without the intervention of the data subject.[58] Moreover, in order to achieve the concept of "privacy by default", the controller should assure that the initial settings of an application disposed to users will allow them to maintain control over what they are posting or sharing with others. The user can choose to reveal more information than the ones needed for his/her processing of personal data, but he/she should to this wittingly, not just because of some initial settings, which were the application's defaults.[59]

3.4. The notification of breaching personal data security

Nowadays, the obligation to notify the breach of data security is applicable only for specific categories of data controllers. Thus, providers of public network services or electronic communication services must notify the supervisory authority regarding the breach of personal data, no later than 24 hours after detecting the breach of data security, when this is possible.[60]

Notifying the Supervisory Authority. GDPR extends this obligation to all personal data controllers. Beginning with 25.05.2018, in case of a personal data breach, the controller shall, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.[61] At

[57]Guide for the implementation of the General Data Protection Regulation for controllers, published on ANSPDCP website (http://dataprotection.ro/?page=Regulamentul_nr_679_2016) (consulted on 1.10.2017).
[58] Art. 25, para. 2 GDPR.
[59] New Regulation (EU) 2016/679 applicable from 25th May 2018 - Novelties (Flyer) published on ANSPDCP website (http://dataprotection.ro/?page=Regulamentul_nr_679_2016) (consulted on 1.10.2017).
[60]http://www.dataprotection.ro/?page=Ghid%20pentru%20formular%20tipizat%20Regulament%20(UE)%20611/2013&lang=ro (consulted on 1.10.2017).
[61] Art.33 para. 1 GDPR.

the same time, the processor shall notify the controller without undue delay after becoming aware of a personal data breach.[62]

Therefore, in order to establish the notification obligation we must be analyse the likelihood of the breaching to generate a risk for the natural persons' rights and freedoms. In order to establish this aspect, we shall take into consideration criteria such as the type of breach, nature, sensitivity and volume of the processed data, the severity of the consequences, the number of affected persons.[63]

The notification of the personal data security breach will contain at least:[64]

a) description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) description of the likely consequences of the personal data breach;
d) description of the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. [65]

The information of the data subject. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.[66]

The communication to the data subject shall not be required if any of the following conditions are met:[67]

a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise;
c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so.[68]

Therefore, the new regulation requires that in this last case of personal data breach the focus be on protecting individuals and their personal data. So, the supervisory authority can be consulted about the necessity of informing data subjects in case of personal data breach. Also, controllers and processors are therefore encouraged to plan in advance and put in place processes able to detect and promptly contain a breach, and to assess the risk for data subjects.[69]

---

[62] Art.33 para. 2 GDPR.
[63] "Article 29" Data Protection Working Party -,,Guidelines on Personal data breach notification under Regulation 2016/679, adopted at 03.03.2017, p.20-22.
[64] Art. 33 para. 3 GDPR.
[65] Art.33 para. 5 GDPR.
[66] Art.34 para. 1 GDPR.
[67] Art.34 para. 3 GDPR.
[68] Art.34 para. 4 GDPR.
[69] Working group, "Article 29" for data protection-,,Guidelines on Personal data breach notification under Regulation 2016/679, adopted at 03.03.2017, p.4-5.

3.5. The personal data processor[70]

Where processing is to be carried out by a processor, he/she shall offer guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the GDPR requirements. Adherence of a processor to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate sufficient guarantees for the implementation of appropriate technical and organisational measures.

Processing by a processor shall be governed by a contract or other legal written act, including by electronic means, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a) processes the personal data only on documented instructions from the controller;
b) ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
c) takes all measures required for data security;
d) respects the conditions referred to engaging another processor;
e) taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;
f) at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies;
g) makes available to the controller all information necessary to demonstrate compliance with his/her obligations.

Therefore, the new regulation imposes a more detailed contract between data controller and processor.

3.6. Records of processing activities

As a novelty, GDPR imposes through art. 30 that **every controller** shall maintain a record of processing activities **under its responsibility.**

This record should contain the following information:[71]

a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
b) the purposes of the processing;
c) a description of the categories of data subjects and of the categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and the documentation of suitable safeguards;
f) where possible, the envisaged time limits for erasure of the different categories of data;
g) where possible, a general description of the technical and organisational security measures.

Moreover, according to GDPR, **every processor's representative** shall maintain a record of all categories of processing activities carried out **on behalf of a controller**, containing:[72]

[70] Art. 28 GDPR.
[71] Art.30 para. 2 GDPR.
[72] Art. 30 para. 1 GDPR.

a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
b) the categories of processing carried out on behalf of each controller;
c) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and documentation of suitable safeguards;
d) where possible, a general description of the technical and organizational security measures

Therefore, we can conclude that a processor who carries out personal data processing also in its own behalf will have to keep two records, one for the processing activities done for the controller and the other for the activities done on its own behalf.

The records shall be kept in writing, including in electronic form and shall be made available to the supervisory authority on request.[73]

Exceptions: According to GDPR[74] the obligations regarding the mentioned records shall not apply to an enterprise or an organisation employing less than 250 persons. However, this obligation will be applicable if (i) the processing carried out is likely to result in a risk to the rights and freedoms of the data subjects, or (ii) the processing includes special categories of data or personal data relating to criminal convictions and offences.

The obligation to keep processing records and the obligation to assess the data protection impact will replace the present obligation to notify the processing to the supervisory authority.[75] Thus, it was decided to drop out the notification obligation of the controllers, and to replace it with a set of obligations for operators, which shall make them more responsible and assure a high level of personal data protection.

3.7. Transferring data in countries outside EU

Nowadays, Law 677 establishes under art. 29 the conditions of the transfer of personal data abroad, as follows:

"(1) The transfer to another state of the data that are subject to processing or destined to be processed after the transfer may take place only if the Romanian law is not breached, and ***the destination state ensures an adequate level of protection level.***

(2) The protection level will be evaluated by the supervisory authority, taking into account all the circumstances in which the transfer is to be performed: especially the nature of the data to be transferred, the purpose of the processing and the period of time proposed for the processing, the state of origin and the state of destination, as well as the legislation of the latter state. If the supervisory authority considers the protection level offered by the state of destination unsatisfactory, it may order the cancellation of the data transfer.[…]

(4) The supervisory authority may authorise the data transfer to another state which does not have at least the same protection level as the one offered by the Romanian legislation, provided that the ***data controller offers enough guarantees*** *regarding the protection of fundamental individual rights. The guarantee must be established through contracts signed by the data controllers and the natural or legal person(s) who have ordered the transfer.''*

The new regulation describes the aspect of transferring data outside EU establishing that, once GDPR enters into force, the personal data transfer to third countries or international organizations located outside EU, will be done in the following situations:

[73] Art. 30 para. 3 and 4 GDPR.
[74] Art. 30 para. 5 GDPR.
[75] The notification cases were significantly reduced as a consequence of adopting the Decision no. 200/2015 for establishing the cases of personal data processing for which a notification is not necessary, and for modifying and repealing some decisions.

1. When there is a decision of the Commission[76] which stipulates that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation.
2. The controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.[77] The appropriate safeguards may be provided, without requiring any specific authorisation from a supervisory authority, by:
   a) a legally binding and enforceable instrument between public authorities or bodies;
   b) binding corporate rules in accordance with the competent supervisory authority;
   c) standard data protection clauses adopted by the Commission or adopted by a supervisory authority and approved by the Commission;
   d) an approved code of conduct by the supervisory authority, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
   e) an certification mechanism approved by a certification body, together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.
3. In the absence of an adequacy decision or of appropriate safeguards, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:[78]
   a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks
   b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
   c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
   d) the transfer is necessary for important reasons of public interest;
   e) the transfer is necessary for the establishment, exercise or defence of legal claims;
   f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
   g) the transfer is performed from a register which, according to EU or Member State law, is intended to provide information to the public, and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.
4. Where a transfer could not be based on a provision from points 1-3, mentioned above, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.[79]

[76] Art.45 GDPR.
[77] Art.46 GDPR.
[78] Art.49 GDPR.
[79] Art.49 GDPR.

3.8. Penalties

GDPR stipulates severe penalties for breaching its provisions by the controller, as follows:

A. Infringements of the following provisions shall be subject to administrative fines up to **10 000 000 EUR**, or in the case of an undertaking, up to **2 %** of the total worldwide annual turnover of the preceding financial year, whichever is higher[80]:
   a) the obligations of the controller and the certification body related to underage subject's consent, to processing that do not need identification, to "privacy by design" and "privacy by default" concepts, to processing activities records, to processing security, to data protection impact assessment, to DPO, to certificates and also to certification bodies;
   b) the obligations of the certification body;
   c) the obligations of the monitoring body.

B. Non-compliance with the following provisions, attracts administrative fines up to **20 000 000 EUR**, or in the case of an undertaking, up to **4 %** of the total worldwide annual turnover of the preceding financial year, whichever is higher:[81]
   a) the basic principles for processing, including conditions for consent;
   b) the data subjects' rights (information right, access right, rectification right, the right to be forgotten, data portability right, opposition right);
   c) the transfers of personal data to a recipient in a third country or an international organization;
   d) any obligations pursuant to Member State law;
   e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority.

Moreover, beside these fines, the supervisory authority, in the exercise of its powers, may adopt the following coercive measures:

a) to issue warnings to a controller or processor that the intended processing operations are likely to infringe the provisions of GDPR;
b) to issue reprimands to a controller or a processor where processing operations have infringed the provisions of GDPR;
c) to order the controller or the processor to comply with the data subject's requests to exercise his or her rights pursuant to GDPR;
d) to order the controller or processor to bring processing operations into compliance with the provisions of this GDPR, where appropriate, in a specified manner and within a specified period;
e) to order the controller to communicate a personal data breach to the data subject;
f) to impose a temporary or definitive limitation including a ban on processing;
g) to order the rectification or erasure of personal data or restriction of processing and the notification of such actions to recipients to whom the personal data have been disclosed;
h) to withdraw a certification or to order the certification body to withdraw a certification issued, or to order the certification body not to issue certification if the requirements for the certification are not or are no longer met;
i) to order the suspension of data flows to a recipient in a third country or to an international organisation.

Taking into consideration the severity of these coercive measures, which can be added to the fine, but also their potential effects over the controller's activity, their consequences can be more drastic than paying the maximum fee.

[80] Art. 83 para. 4 GDPR.
[81] Art. 83 para 5 GDPR.

4. From the perspective of the supervisory authority

4.1. Proximity to the data subject, the "One Stop Shop" concept and cooperation between Supervisory Authorities

Taking into consideration the general applicability of GDPR in the whole EU, art.77 stipulates the data subject's right to lodge a complaint with a supervisory authority, especially in the member state where the data subject has his/her common residency, job or where the supposed breach took place, if he/she considers that the personal data processing caused him/her prejudices.

At the same time, proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.[82] Therefore, the supervisory authority from the Member State of the data subject will be a contact point, when the controller is located in another Member State. In this way, the implication of the supervisory authority from the Member State where the data subject is located is assured in the process of adopting a decision, in the case of a controller located in another State Member.[83]

Regarding the controllers, if the processing of personal data takes place in the context of the activities of an establishment of a controller and the controller is established in more than one Member State, or if the processing taking place in the context of the activities of a single establishment of a controller in the EU substantially affects or is likely to substantially affect data subjects in more than one Member State, the supervisory authority for the main establishment of the controller or processor, or for the single establishment of the controller or processor should act as lead authority. ("**One–Stop-Shop concept**").[84] This authority should cooperate with the other authorities concerned, because the controller or processor has an establishment on the territory of their Member State, because data subjects residing on their territory are substantially affected, or because a complaint has been lodged with them.[85]

In the case of a cross-border data processing, the main supervisory authority cooperates with the other supervisory authorities, in the attempt to reach a consensus and to assure mutual assistance. The lead supervisory authority and the supervisory authorities concerned shall exchange all relevant information with each other.[86]

4.2. The competences of the supervisory authority

GDPR details the competences of the national supervisory authorities and separates it in three categories:

1. Investigative powers
2. Coercive powers[87]
3. Authorization and advisory powers

Amongst the investigative powers there are the followings:[88]

a) to order the controller and the processor, and, where applicable, the controller's or the processor's representative, to provide any information it requires for the performance of its tasks;

---

[82] Art. 79 para. 2 GDPR.

[83] New Regulation (EU) 2016/679 applicable from 25th May 2018- Novelties (Flyer) published on ANSPDCP website (http://dataprotection.ro/?page=Regulamentul_nr_679_2016) (consulted on 1.10.2017).

[84] Art. 56 para. 1 GDPR.

[85] Preamble 124 from GDPR.

[86] Art. 60 GDPR.

[87] See point 2.8 from above.

[88] Art.58 para. 1 GDPR.

b) to carry out investigations in the form of data protection audits;
c) to carry out a review on the issued certifications;
d) to notify the controller or the processor of an alleged infringement of GDPR;
e) to obtain, from the controller and the processor, access to all personal data and to all information necessary for the performance of its tasks;
f) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means, in accordance with EU or Member State procedural law.

Authorization and advisory powers include:[89]

a) to advise the controller in accordance with the prior consultation procedure referred to data protection impact assessment;
b) to issue, on its own initiative or on request, opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
c) to authorize processing after the prior control, if needed;
d) to issue opinions and approve draft codes of conduct;
e) to accredit certification bodies;
f) to issue certifications and approve criteria of certification;
g) to adopt standard data protection clauses;
h) to authorize contractual clauses between controller or processor and controller, processor or data recipient from a third country or international organization;
i) to authorize administrative arrangements between authorities or public bodies, which include enforceable and effective rights for the data subject;
j) to approve mandatory corporate rules.

For the fulfilment of all the attributions established through GDPR for the supervisory authority, the adoption of several national legislative acts that can stipulate specific procedures thoroughly will be needed. Nowadays, there is a legislative proposal to amend Law no. 120/2005 regarding the establishment, organization and functioning of the Romanian Supervisory Authority (ANSPDCP). It establishes for the president of the ANSPDCP the task of monitoring the compliance and application of GDPR, and it details the procedure for the enforcement and compliance of the coercive powers of the ANSPDCP. At the same time, it is estimated that the number of people from the staff within the ANSPDCP will reach 85, from 37, which is the current number.[90]

5. Conclusions

The new data protection legislation brings a number of important changes for all categories of people involved in a personal data processing. Thus, on the one hand, the aim is the accountability of personal data controllers and, on the other hand, to strengthen the rights of the data subject, as well as the introduction of new rights for them.

In order to ensure that a data processing by controllers complies with the new requirements at the time GDPR becomes applicable, the controller should take the following measures:

- to draw up an inventory of all the processing operations it carries out;
- to clearly set out the purpose and basis of the processing;
- to keep only the data strictly necessary for achieving the purpose of the processing;
- to analyse the need to obtain the data subject's consent again, respectively to update the information note;
- to contract a DPO, if the case;
- to consider the need for any data protection impact assessment;

[89] Art.58 para. 3 GDPR.
[90] http://81.181.207.101/frontend/documente_transparenta/72_1504614894_Tabel%20comparativ.pdf (consulted on 1.10.2017).

- to verify the basis of transfers of data to third states or international organizations;
- to adopt/update internal policies in line with the new requirements;
- to develop training programs for the staff involved in the personal data processing.

Bibliography

1. Directive 95/46/CE of the European Parliament and Council from 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data
2. *Regulation (EU) 2016/679 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*
3. Law no. 677/2001 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
4. Guide for the implementation of the General Data Protection Regulation for controllers, published on ANSPDCP website (http://dataprotection.ro/?page=Regulamentul_nr_679_2016) (consulted on 1.10.2017).