THE NEW DATA PROTECTION REGULATION CLAIMS UNDER GDPR

Ana-Elena IUNKER C.GH.
Titu Maiorescu University, Bucharest, Romania, Ph.D.Student
22 Street Dâmbovnicului Tineretului, Bucharest 040441, Romania
Telephone: 0040749112361
E-mail: iunker.ana@gmail.com

Abstract: *After 2 years since The General Data Protection Regulation entered in force, we finally face the day when it starts to apply. May 25, 2018 was the "Z" day regarding Data Protection Laws and Practices.*
The necessity of this regulation is obvious and addresses both the data processed within European Union and the data transfers outside the European Economic Area. GDPR extends the scope of EU data protection law to all foreign companies processing data of EU residents.[1] The regulation highlights the following key requirements: scope, single set of rules, responsibility and accountability, lawful basis for processing, consent, data protection officer, pseudonymization and anonymization, data breaches and sanctions.
The main purpose of the GDPR is protect this important asset called personal data. First fines within this new legal background were imposed and it is important for all of the data controllers to ensure their compliance towards the GDPR.

Key words: *The General Data Protection Regulation; scope; data protection officer, lawful basis for processing, consent, data breaches and sanctions.*

Introduction

Starting with 2012, the European Commission initiated the process of the new legislation regarding data protection. By the end of 2015 the European Parliament, Council and Commission established the novelty for the data protection area, which had the same legal frame in the European Union as a result. This is why they accepted the Regulation to the detriment of the Directive as a final legal basis. The new law, under the Regulation final form was adopted in April 2016 by the Council and the Parliament.

On May 4th, 2016, the European Union Regulation Official Newspaper 679/2016 of the European Parliament and Council of April 27th, 2016 published an article „on the protection of individuals with regard to the processing of personal data and on the free movement of these data and the repealing of Directive 95/46 / EC" (General Data Protection Regulation).[2]

The regulation is a mandatory European Union legislative act that must be applied entirely by each and every single member state of the EU. As the EU states on its

own homepage„unlike a regulation, the directive is a legislative act setting an objective that all the members of the EU must meet, but each of them has the right to decide on how to meet the established objective. The distinctions between the mode of application and the effects of the two types of European legislative acts also shows us why the regulation option is more effective".

The protection of personal data has the following technical cause: the development of information systems. The development of computer systems raises the following issues: memory, communication and intelligence. Computer systems have memory, computer systems allow for easy communication of stored information and information processing in a sufficiently short time for the use of processing results to be effective.

"The Charter of Fundamental Rights of the European Union" only concerns the rights of individuals. So is the art. 8 of the Charter, which provides: "Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by the law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority" [3]

The right to data protection derives from the right to respect for privacy. The concept of private life is associated with human beings. Individuals are therefore the main beneficiaries of data protection. [4] Furthermore, according to the Working Party 29 Opinion, only human beings are protected by European data protection law. The jurisprudence of the ECHR on Article 8 of the ECHCR shows that the complete separation of private and professional life can be difficult.[5]

The GDPR Regulation is structured on 11 chapters that grouped 99 articles and 173 recitals, as follows [6]:

1. „General provisions" (Art. 1 – 4)

2. „Principles" (Art. 5 – 11)

3. „Data subject rights" (Art. 12 – 23)

4. „Processor/Controller" (Art. 24 – 43)

5. „Personal data transfer to third countries/international organizations" (Art. 44 – 50)

6. „Supervisory Authorities from the Member States" (Art. 51 – 59)

7. „Cooperation" (Art. 60 – 76)

8. „Penalties" (Art. 77 – 84)

9. „Specific data processing situations" (Art. 85 – 91)

10. „Delegated acts and implementing acts" (Art. 92 – 93)

11. „Final provisions" (Art. 94 – 99) [7]

1. Regulation (EU) 2016/679 - Scope

Regulation (EU) 2016/679 is directly applicable in all EU Member States, protects the rights of all individuals within the EU and extends the scope also to data controllers working outside the EU in the extent to which their goods and / or services are addressed to persons located within the EU.[8]

Personal data is important in the identification of individuals (Article 4 (1) of the Regulation). [9] Social interaction between people is done through exchange of information; in the absence of information exchange, the functioning of society is unthinkable.

We could say that some of this information allows us to identify the people who interact, but closer to the truth if we observe that most of the information conveyed allows us to identify the person who is talking to them. We can say that society abounds with personal data.

The information allows the holder to act effectively. That is why information is power. Information extracted from personal data is important because it allows profiling. Consequently, they enable active agents to achieve attention management through personalized interactions.

The legal meaning of personal data does not clarify when a person is deemed to be identified. Identifying clearly involves elements that describe a person in a way that he can distinguish himself from all other persons and can be recognized as a natural person. Someone's birth name can be an example of a description element. In exceptional cases, other identifying elements may have a similar effect to the name. As an example, in the case of public figures, it is enough to specify their position, for example, the President of the European Commission.

2. How it works?

The new data protection legislation is a regulation so it will automatically apply to all concerned entities without the need for national legislation, since it is a regulation and not a directive. It replaces Romanian law no. 677/2001 on Data Protection.

It is necessary to implement technical and organizational security measures through which data protection principles can be effectively implemented. It is also necessary to minimize processed data and to ensure safeguards in the processing in order to comply of the Regulation and to respect the data subjectsrights [10].

The protection granted by the GDPR concerns individuals, regardless of their nationality or residence, in respect of the processing their personal data. Therefore, the GDPR confers on individuals more rights, which they can exercise freely with respect to the data processing entities, such as: the right to information, the right of access their personal data, rectification and erasure, the right to restrict the processing, „the right to reuse personal data a.k.a portability", the right to object against using such data.

3. Principles of GDPR

The principles governing the general data protection regulations are:

- Lawfulness, fairness and transparency (linked to fundamental human rights).

- Purpose-limitations (personal data of the subjects needs to respect the well-defined criteria, legitimate purposes, and subsequent processing must not deviate from these purposes); [11]

- Minimizing the collected data

- Appropriate, limited and relevant (this principle makes it clear that any personal data collection needs to be the most relevant to what is the purpose in which they are processed);

- Verifying the accuracy of data and updating it;

- Storage-related limitations (data must be kept as long as needed for the underlying storage. Longer storage periods are exceptions associated with public archiving, research or statistical activities);

- Integrity and confidentiality - data security (security processing Ex ISO 27001 certifications);

4. Lawfulness of processing

Article 6 provides the scenarios in which data controllers are allowed to process individual's personal data:

(a) the data subject has given a valid consent regarding the granular purpose of processing their personal data;

(b) the data is vital for the signing of a contract;

(c) the controller has a legal obligation while processing that personal data;

(d) there is a vital interest of the personal data subject or another natural person. Ex when calling for an ambulance;

(e) there is a public interest for processing the personal data;

(f) there is legitimate interests when processing such data" [12]

There is no time limit specified in GDPR, for how long the consent will be valid. The consent timeframe will be contextual and the initial consent scope will depend as expectations of the person concerned. If processing operations change or evolve considerably, the initial consent is no longer valid. In this case, a new consent must be obtained.

Article 6 (f) is provided as the last option among the six grounds that allow the personal data to be processed lawfully. It requires a comparative test: what is necessary as legitimate interest of the operator (or third parties) must be balanced against the interest or fundamental rights of the data subject.

Article 6 from the General Data Protection Regulation is considered to be one of the most important because it is drafting the scenario when any individual can process personal data. It is clear that if anyone can link their processings to any of the cases listed above, there is la lawful processing of such data.

4. Who is evaluating?

In Romania, the National Supervisory Authority called ANSPDCP [13] will carry out checkings and apply sanctions on behalf of the EU.

5. Special features for a valid Consent

As for the consent, the former Working Party 29 (EDPB now) has given a general understanding of how this consent should be obtained from the natural person. Consent should, inter alia, be given unequivocally, informed and free of charge.

Article 4 (11) The GDPR defines a valid consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" [14]

Consent must be given through an action (unequivocal declaration or action). This means that the simple reference currently available on many sites that says "by continuing to use this site you agree to processing your data" is no longer enough.

Thus, consent must be given by an unequivocal action which is a free expression, specific, informed and clear expression of the person's agreement. Such actions may be written statements, including in electronic form, including ticking a box when the person visits a site.

For the manifestation to be specific, informed and clear, the operator to process the data must provide clear, simple and transparent information respecting the main purpose of that processing, the basis of the processing, the time for which the data is processed, and its right to take back their consent.

The subject of the data must also be informed of the data controller identity and data protection officer, the data recipient and any interests and intentions to transfer them to third countries. Be careful: If you need multiple purposes, consent must be given for each of them!

There is also a very important clause in the official guideline regarding the imbalance of powers. In practice this case can be translated as a typical situation where a aanager is going to ask his employees to consent on installing CCTV cameras in their office. This is clearly an imbalance of powers because in most of the cases those employees are going to be literally forced to accept anything their direct manager is going to ask for. Ideally when we talk about personal data processed as an employment form, we should not use the consent as a valid way of using personal data.

Working Party 29 also stated that there are also other cases beside the employment context, such as public authorities and any other situation when the data subject is not able to express a real choice without feeling pressured, intimidated or significant negative consequences. In these cases consent is not going to be given free so it is not going to be valid.

There is another important factor when any processing is going to be based under the consent form and that is the granularity of the consent. The meaning of this lies in the core of this Regulation. Any data subject must be informed about how his/hers personal data is going to be used. So, specifically for the consent, the data controller must be able to demonstrate that he has obtained a different consent for each and every final purpose of that processing. For example, if there is a consent form where it is clearly stated that the subject is accepting to receive marketing informations by email, the controller should only use that database to send the requested information to the people. But, in case that data controller wants to transfer these data to thers, he/she should have to obtain a different consent for this new purpose of the processing. Shortly, the data subjects have to be clearly informed about whatever is going to happen with their data.

The controller should also be able to demonstrate that the consent can be withdrawn at any moment without any negative consequences. Moreover, the consent must be withdrawn as easy as it was adressed and should always be free. As an example, we cannot ask someone to call (costly phone call) in order to withdraw their consent. It should be as easy as checking a box, filling a form or sending an email.

When asking for consent, controllers should not use pages of technical language because it is not going to be a valid form of informative measures regarding the usage of personal data. The language used should be accessible, easy to understand and clear.

Maybe the most important aspect of the constent is the way the data controller is going to be able to demonstrate it. In other words we cannot ask someones consent verbally when using the personal data because we are not going to be able to prove so. Any written statement as acceptable under GDPR as a valid consent.

There are cases when special legal requirements are asking for the usage of personal data. For instance, for security reasons, every tourist that is going to rent a room in the hotel will have to fill a form regarding his/hers personal data. In such cases, the law is specifically stating which data should be collected and what is going to happen with it. In most of the cases, these papers are being sent to the police station.

Conditions of a valid consent

a. It must be free

Thus, according to the Regulation, the consent will not be freely expressed if:

- the data subject does not really have the freedom of choice or is unable to refuse or withdraw his consent without being harmed;
- there is an obvious imbalance between the data subject and the operator, especially if the operator is a public authority. For example, this requirement will question the validity of employees' consent for data processing by employers. In Romania, in general, employers process data based on consent. As such, they will have to consider if, after May 25, 2018, they can still rely on the consent of the employees one of the theme of data processing;
- the granting of consent does not allow it to be given on different data processing operations, although this is appropriate in the particular case

b. It has to be specific

A very broad consent, given for general / indeterminate purposes, is not valid. To be considered valid, operators must clearly identify the purposes of the processing, and the consent must cover all processing activities carried out for the same purpose. In addition, if data processing is for multiple purposes, consent should be given for each purpose separately (granular)

In case the data processing is done for scientific research purposes, it is not mandatory to fully identify the purpose of the processing that is the object of the research, being sufficient that the data subjects can only consent for certain research areas identified by the operator. However, the requirement regarding the granularity of the consent should be respected, that is to allow the data subject to give his consent only for certain fields of research or parts of the research projects (to the extent permitted by the intended purpose).

c. It must be informed
The regulation provides that any processing of personal data should be carried out in a transparent manner by informing the data subjects about the existence of data processing and the conditions under which the data are processed.

Thus, the information and communications regarding data processing must be easily accessible and easy to understand, using a simple and clear language. Information notes with very technical terms do not comply with the requirements of the regulation and will attract invalid consent.

Thus, when drafting the information notes displayed on web pages / online platforms, operators must take into account the language of each jurisdiction in which the data subjects are located, in order to avoid any possible discussions regarding the validity of the consent.

d. It must be unequivocal
The regulation makes some clarifications regarding the meaning of unequivocal consent. Thus, in order to be considered unequivocal, it must take the form of a statement or an action that clearly shows the intention of the data subject to give his consent.

What are the actions that clearly show the intention of the person to give his consent?

Below are some examples provided by the Regulation:

a) ticking some boxes when the person visits a web page,

b) choosing the settings for the information society services; or

c) any other statement or action that clearly indicates in a given context the acceptance of the proposed processing by the data subject.

In the general hypothesis provided in letter. c) the following examples could be included

- providing the e-mail address in the context of creating an account on an online platform, in a box where it is indicated that the provision is optional, and under the box a short message such as "e-mail address will be used for to send commercial communications with our products and / or services:

- the processing of body size data by a tailor, if the data subject requested the creation of a clothing item and thus provides the body dimensions; it could be considered that there is the consent of the data subject and if this allows the tailor to take the bodily dimensions necessary to create the clothing object.

It is important to note that the Regulation expressly provides that the absence of a response or action cannot be considered valid consent. Also, the boxes previously

checked in the web pages or the software applications will not be able to be invoked as viable mechanisms of expressing the consent.

Finally, the Regulation provides that, if the statement of the data subject relates to several aspects, the request for consent must be presented in a form that clearly differentiates it from the other aspects.

7. Personal data /sensitive data

Special categories of personal data are strictly delimited by law: race, ethnicity, political orientation, religion, philosophical or similar beliefs, sindical status, health data, sex life data and so on. In addition, sesitive data is considered:

• Personal data that is going to immediately identify any natural person such as National Identification Number (CNP)

• personal data relating to criminal offenses or contraventions

8. Rights of the data subjects

- Right of access (art. 15) it is possible to ask the operator in writing, under his/her signature and date, to communicate if he / she is processing the data, for what purpose, what data, who he / she reveals, where they were collected, automatic machining mechanisms use.

- Right to rectification (art. 16) it may be required by the operator in writing, under signature and date, to rectify or update the data, or to block the data processing, erase, anonymous data if it has illegally processed or communicated to third parties to whom your data has been disclosed, any requested operation (rectification, update, deletion, etc.)

- Right to be forgotten (art. 17) - individuals will have the right to require an operator to delete records of data related to them, provided there are no legitimate reasons for such data to be retained; Individuals may request that their data be "deleted" when there is a problem related “to the lawfulness of the processing” or the withdrawal of the consent.

- The right to be notified in case of data security breaches (art 19): companies will be obliged to immediately notify individuals of significant breaches of data security.

- The right to data portability and transfers the data to another provider (art 20) - customers will be entitled to request an electronic copy of their data undergoing processing and transmission of data required directly to another operator.

- The right to restriction (art 18): it may be required to require the operator, in writing, under his/her signature and date, not to process the data for direct marketing purposes or to disclose it to third parties for that purpose.

- "Automated decision-making, including profiling" (art 22): this right refers to the option that a natural person is not going to be subject to individual automated decisions: the operator may be required to withdraw, cancel, re-evaluate a decision he has taken solely by using the automatic means by which he assesses his professional competence, credibility or behavior under certain conditions.

Example: An important example of making automated decisions is the assessment of solvency. To take any decision on the future creditworthiness of a client, some data is collected from the client and combined with data on the person concerned from other sources such as credit information systems. The data is automatically listed into an evaluation algorithm, which calculates a total value representing the solvency of the client potential.

The data subject has also the following rights:

- „The right to be informed" (free of charge): by the operator, when the data is collected or at the earliest at the earliest, before disclosing to third parties: who is the operator, for what purpose does your data work, to whom could reveal in trhe case you have to provide him with all the required data and what the consequences of a refusal are, what rights you have and how you can exercise them.

- „The right be inforbed about the personal data processing registry" (free of charge): it can be checked whether an operator has notified ANSPDCP that it processes personal data, including online, by accessing www.dataprotection.ro.

- „The right to contest to the courts" (free of charge): the operator who has failed to comply with the rights or has caused damage by illegally processing the data may be sued.

9. Why it is the Regulation so important?

The regulation is important in terms of how it governs liability and because of very severe sanctions.

Its primary objective is to protect and empower all EU citizens in data privacy issues and to transform the manner in which organizations approach data privacy. It does not apply only to EU organizations but all organizations that are processing personal data of the subjects residing in European Union.

Along with this increased territorial scope, meaning an extra-territorial applicability, the new regulations bring:

- new conditions for consent, that „must be clear and distinguishable from other matters and provided in an intelligible form, using clear and plain language".

- modifications on data subject rights as breach notification, right to access, right to data, data portability, privacy by design and data protection officers.

10. Sanctions

For disclosure of data protection obligations:

- 10 (ten) million or „up to" 2% of global turnover; For violations of the basic principles of data processing (proportionality, legitimacy, consent, etc.), the rights of data subjects (access, the right to be forgotten, etc.), international transfers of data or non-responsive with a data protection authority measure:

- 20 (twenty) million or „up to" 4% of global turnover.

11. Famous fines

Based on a report published by the European Data Protection Board on their website [15] we can take a look at how the National Supervisory Authorities enforced the New Data Protection Regulation within the EU.

a) By far, the most important fine under the GDPR was imposed in the UK for British Airways, aprox. 230 million euros. Following an extensive investigation, the Office of the Information Commissioner (ICO) announced its intention to sanction the British airline British Airways with a fine of 183.39 million pounds (230 million euros) for violating the General Protection Regulation Data (GDPR). After a cyber attack, hackers stole data from about 500,000 customers, according to information available on the ICO website. The airline declared itself "surprised and disappointed" by the fine. ICO said this is the largest sanction it has ever given and the first to be made public under new European personal data rules (GDPR).

The incident was made public on September 6, 2018, and airline representatives initially claimed that about 380 thousands transactions were affected. British Airways said the information included names, e-mail addresses, and other info such as credit card information, such as credit card numbers, expiration dates, and the three-digit CVV code found on the back of credit cards, although the airline has stated that it did not store CVV numbers.

b) Marriott International, Inc. (110,390,200 euros) - UK

In second place it is the fine also applied by ICO to Marriott International, Inc. in the amount of 110,390,200 euros (£ 99 million) for infringement of the same art. 32. The fine is not yet final according to the ICO release dated July 9, 2019. In the

Marriott case, a security breach led to the exposure of 339 million customer sign-ups.

The Marriott security breach came after Starwood hotel systems were compromised in 2014. Marriott acquired Starwood in 2016, but customer information exposure was only discovered in 2018.The ICO investigation found that Marriott did not make every effort to secure the systems, after buying Starwood. Marriott has cooperated with the authorities since the occurrence of these events.

c) Google inc. (50,000,000 euros) - France

The third fine of 50,000,000 euros was applied in France by the French Data Protection Authority a.k.a CNIL to Google Inc. for the violation of the article 13, article 14, article 6, article 4, article 5, from the General Data Protection Regulation according to the CNIL communiqué of January 21, 2019. Google has been accused of lack of transparency, inadequate information provision and not obtaining any legal consent for the marketing purpose..

The investigation started in June 2018 on the complaints of the data subjects and lasted about 7 months. It is rellevant to note that the complaints arose immediately after the new regulation 679/2016 came into effect. Verifying compliance with data protection legislation was accomplished by analyzing a user's browsing model and documents that the user can access when setting up a GOOGLE account while configuring a mobile device that uses Android.

CNIL noted that the way the information presented to users is structured is not complying with the GDPR. Essential information, such as data processing purposes, data storage periods, or categories of personal data used to personalize your ads, are over-served in multiple documents, with buttons and links you need to click to access additional information.

d)The Hague Hospital (460,000 euros) - Netherlands

In the Netherlands, the Dutch Supervisory Authority sanctioned The Hague Hospital with a fine of 460,000 euros for violation of art. 32 GDPR, according to the press release dated July 16, 2019. The Haga Hospital was fined for failing to comply with safety and security measures regarding access to patient records.

The national authority started the investigation due to information that several staff members were able to access the medical file of a hospital patient, a public person, although they were not involved in his treatment. The authority applied a fine of 460,000 euros for lack of sufficient security guarantees regarding access to sensitive data, respectively medical data.

In addition to the fine of 460,000 euros, the authority applied to the hospital and complementary (corrective) measures of alignment with the GDPR norms. Thus, the authority forced The Hague Hospital to, by October 2, 2019, improve patient data security. If the hospital does not comply until then, the authority will enforce the damages-comminers: 100,000 euros to be paid every 2 weeks, up to a maximum of 300,000 euros.

e) FRANCE - Sergic, PORTUGAL - Barreiro Montijo Hospital Center (400,000 euros)

- In France, CNIL applied a fine of 400,000 euros to Sergic for violating Articles 5 and 32 GDPR. Sergic was accused of lack of data security measures and failure to observe the storage time.

- The same amount was fined a public hospital by the Portuguese Data Protection Authority (CNPD) for violating Articles 5 and 32 GDPR. Centro Hospitalar Barreiro Montijo was accused of unauthorized access to sensitive data and the lack of internal procedures to ensure data protection.

f) Unicredit Bank Romania (130,000 euros) [16]

The National Supervisory Authority has finalized an investigation at Unicredit Bank and found that it violated the provisions of the GDPR under the aspect of natural persons personal data.

The sanction was applied to Unicredit Bank S.A. „as not being able to secure the usage of personal data both at the time of establishing the means of processing and in the processing itself, intended to effectively implement the principles of data protection, such as minimizing data, and integrate the necessary guarantees in the processing, in order to respect the GDPR requirements.

The sanction was applied as a result of a notification of the National Supervisory Authoritu, indicating that the data regarding the CNP and the address of the persons who made payments to Unicredit Bank S.A., through online transactions, were disclosed to the beneficiary of the transaction, through the account statement / details forms.

The case involving big names such as Google, Facebook (under the old directive), British Airways or Marriott International provides clues about the current state of data security, assuming that the company's financial strength allows it to implement the most effective measures.

However, the reality shows that there are difficulties in interpreting the rules and problems can arise in the most varied fields. The presentation below gives an overview of the affected industries (company names are presented based on data availability):

Financial-Banking: Romania (Unicredit Bank SA), Hungary (bank, debt collector), Bulgaria (banks), Czech Republic (brokerage agency), Spain (debt collector)

Medical: Netherlands (The Hague Hospital), Portugal (Barreiro Montijo Hospital Center), Cyprus (hospital), Bulgaria (medical center)

Authorities: Norway (Bergen Municipality), Malta (Lands Authority), Hungary (City Hall), Belgium (Mayor), Germany (Police Officer)

Hotels: United Kingdom (Marriott International, Inc); Romania (World Trade Center Bucharest SA)

Telecommunications: Spain (Vodafone Espagna), Bulgaria (telecommunications service provider)

Technology, software: France (Google inc.), Denmark (IDdesign A / S)

Political parties: Italy (Italian political party 5 Star Movement), Hungary (political party)

Sport: Spain (Professional Football League - LaLiga), Poland (Sports Association)

Media: Germany (N26), Cyprus (newspaper)

Aviation companies: United Kingdom (British Airways)

Real estate: France (Sergic)

Energy: Spain (Endesa)

Without claiming to be exhaustive the list above indicates sensitive areas and confirms that data protection becomes an issue that should be concerning to any company or private person, in the exercise of a function or not.

Conclusion

According to GDPR, both data operators and their authorized processors will be held responsible for the personal data they process. However, they have different obligations, so it is crucial to draw a clear delimitation. In short, the operator determines the purpose of that processing, while the person empowered as a processor is the one who carries out the actual processing.
The most important consequence of the status of operator or person empowered by the operator as processor is legal responsibility for compliance in accordance with data protection legislation. Therefore, only those who can be held accountable under applicable law can assume these functions
The legislative adoption of EU General Data Protection Regulation, proves that the EU authorities recognize the new realities on the individual rights and liberties and tries to solve possible conflicts in current legislation. The text of the Regulation,

even though not explicitly put it, brings together in the effort to protect personal data of the citizens.

We stronly consider that each and every single time when a data controller has any problems regarding the uderstanding of the new Regulation they should consider the Working Party 29 Guidelines and the EDPB papers established especially to solve the dorctrinary inconsequences.

In our opinion, each data controller should firstly understand the data flows used in his activity, and then to map the risks to which he is exposed, to map these data. From our point of view, this process is specific to each data controller, as the degree of use of personal data differs from one data controller to another. Also, each field of activity has its own specific. In order to comply with a minimum legal requirement, the data controller should train his employees so that they can get a minimal compliance by respecting the data subjects rights. We strongly believe that the data controllers compliance is representing just the tip of the iceberg. The most important aspect of it should be the awareness of the new legislation and corporations should invest time and knoledge in skilled data protection officers in order to comply with the novelty of this updated legal field.

Also, in order to comply with the Regulation, data controllers have to prove that they have obtained a valid consent from the data subjects. Therefore, apart from meeting the conditions addressed by the Working Group 29 in the Guidance on the Validity of Consent, it must always be granted by an action and not by an inaction, especially when talking about completing the online forms.

References

[1] Working Party 29 Guideline on the territorial scope: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf
[2] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679
[3] The Charter of Fundamental Rights of the European Union: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679
[4] Working Party 29 official guideline interpretation
[5] Furthermore explaination: Irina Alexe, Nicolae-Dragoş Ploeşteanu, Daniel-Mihail Şandru (coord.), *Protecţia datelor cu caracter personal. Impactul protecţiei datelor personale asupra mediului de afaceri. Evaluări ale experienţelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679*, Ed. Universitară, București, 2017.
[6] https://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf
[7] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[8] General Data Protection Regulation 679/2016 GDPR: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32016R0679&from=EN
[9] General Data Protection Regulation 679/2016 GDPR: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32016R0679&from=EN
[10] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679
[11] https://slidelegend.com/data-protection-laws-of-the-world_59cfe0721723dd38fe719be0.html
[12] WWW.DATAPROTECTION.RO
[13] General Data Protection Regulation 679/2016 GDPR: https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:32016R0679&from=EN
[14] Simona Șandru, *Protecția datelor personale și viața privată*, Ed. Hamangiu, București, 2016; Gabriela Zanfir, *Protecția datelor personale. Drepturile persoanei vizate*, Ed. CH. Beck, București, 2015
[15] https://edpb.europa.eu/news/national-news_en
[16] https://www.dataprotection.ro/?page=Comunicat_Amenda_Unicredit&lang=ro