CREDITFORTE

REGULATION (EU) 2616/759 OF THE EUROPEAN PARLIAMENT AND COUNCIL OF 27 APRIL 1016 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)

Dr Gábor Saly
Managing Director

INTRODUCTION

Definition of personal data

Personal data are such information that can be linked to the identification of the individual or make his/her identification possible. The range of these data is very broad: e.g., one kindergarten teacher shared a photo of the children following a celebration in the kindergarten, and, among them one of a child on which only his legs could be seen only, the face not. A parent still asked for the photo to be deleted, as the child had such special shoes that he could be identified based on them. As the example shows, personal data are very diverse. There are apparent and, thus, easily identifiable among them, but there are also other, discrete and inconspicuous data which make an individual identifiable. Any data can be declared a personal data if it allows the direct or indirect identification of a living person.
Personal data can, among others, be used for identifying individuals and if these are published it shall be more difficult to protect one's privacy. The sharing of personal data poses the same dilemma. To be on holidays on the Adriatic Sea is, by all probabilities, an exciting adventure that people want to share with their friends and acquaintances. They would not like, however that the hotel where they stayed shared the information collected about them, as this could, for many reasons, spoil the trip. The purpose of the regulation on the protection of personal data is to protect **natural persons**. The General Data Protection Regulation does not provide protection to legal entities, such as, for example, firms, societies, clubs, member organizations, companies or others.
The EU has recognized the importance of personal data in an ever-expanding business world. The opportunities are countless. E.g., by knowing a phone number or a Google account all our equipment and accounts can be accessed. If we have lost or shared any such information, anyone can have access to data bases containing our personal data. In view of the fact that in the majority of the cases we accept the conditions of use of a website or service in a way that we do not even know we do accept, what data we have disclosed concerning ourselves. who can obtain these data and what are the costs we have undertaken, for how long, on what basis, for which purpose, etc., or can our data be used, the European Committee has decided that it shall regulate in the future this enormous area with a view to protect customers.

Terms

Processing: operations performed on personal data. According to the definition the storage of the personal data "without using them" also classifies as processing.
Profiling: the use of personal data for the evaluation of certain aspects in connection with the studied individual. E.g., health insurers may analyze the personal data, can calculating the health risk or marketing agencies may use profiling for sending you offers by e-mail, based upon the websites you have visited (your preferences).
Pseudonymisation: the processing of the personal data in such a manner that they can no longer be attributed to a specific data subject. E.g., the data of the individual are stored in several separate files under different names hindering thereby a hacker obtaining a full set of information on the given person by hacking one single file.
Data controller: means the natural or legal person who or which determines the purposes and means of the processing of personal data. E. g., Firm "A" sells electronic equipment, and uses the e-mail services of Firm "B" for sending e-mails to customers. In this case, with regard to the e-mail services Firm "A" is the data controller and Firm "B" the data processor. It is important to make distinctions between the two as different rights and obligations belong to the different entities/roles.
Data Processor: means the natural or legal person who processes personal data on behalf of the data controller.

Sensitive data – according to the General Data Protection Regulation the sensitive personal data are a "special category of information". The following belong here: trade union membership, religious beliefs, political opinions, race and sexual orientation.
Misuse of personal data: infringing the security rules which leads to the accidental or unlawful destruction, loss, modification, unauthorized publication of or access to transmitted, stored or otherwise processed personal data. The offence of the breach of personal data is committed, for example, if the data base of the data controller or processor is hacked and the personal data are stolen.
Data Protection Impact Assessment (DPIA): means a process helping the organizations to identify and minimize the data protection risks of new projects or policies

ASCOPE OF APPLICATION OF THE GENERAL DATA PROTECTION REGULATION

This Regulation regulates the processing of personal data in the context of the activities of EU data controllers and processors irrespective of whether processing shall take place in the EU or elsewhere. The Regulation does not cover data processing by natural person persons in the course of their personal or household activities.

KEY PRINCIPLES

The General Data Protection Regulation follows the following key principles when assessing the processing of personal data:

- **lawfulness, fairness and transparency** of the processing of personal data
- **purpose limitation**: personal data can be collected only for the set unambiguous and lawful purposes and cannot be processed in a way not consistent with these
- **data minimisation:** only data necessary for the processing shall be relevantly collected
- **accuracy:** ready-to-date data, rectified without delay
- **storage limitation:** the data shall be stored in a form that allows the identification of data subjects only as long as it is necessary for the purpose of data processing
- **integrity and confidentiality:** to secure an adequate level of security for the personal data
- **accountability:** the data controller is responsible for observing the rules of the General Data Protection Regulations and for certifying this.

LEGAL BASIS OF DATA PROCESSING

There are 6 legitimate legal bases for the processing of personal data, namely:

1. approval of the data subject, consent
2. contractual obligations
3. legal obligations
4. protection of the vital interests of natural person
5. public interest
6. rightful interest.

The majority of legal bases cited above have existed also before the General Data Protection Regulation has come into force; the most important the changes are with respect to the consent by the data subject.

Consent by the data subject

Consent means that the data subject consents to his/her personal data to be processed for one or more specific purposes. If the individual consents to data processing without being informed of the purpose fully and understandably, then the consent cannot serve as legal basis for the processing as, according to the definition, it was not given voluntarily in this way, as what processing means is not well-defined and unambiguous in this case. Therefore, consent shall meet the following criteria:

1. It shall be given uninfluenced, from the data subject's own will
2. It must be accurately defined, with the data subject being informed and the limits of the consent being made unambiguous
3. Obviously, the private person should know the purposes of data processing so that he/she could decide whether he/she is willing or not to share his/her personal data for that purpose. Such can be, e.g., when he/she gives his/her consent by clicking to the checkbox on a website visited, selects the technical settings of services associated with the information society, or makes other declarations or shows attitudes which are the clear sign in this context of the data subject's consent to the processing of his/her personal data.

Rightful interest:

"Rightful interest" is the most flexible from among the six legal bases: it expresses the ratio of the rightful interests and freedoms of the data controller and the data subject. The burden of proof lies with the data controller, who must prove the supremacy of his rightful interests as compared to the implicit general interest of the data subjects. In the majority of the cases it is necessary to examine whether the interests of the data controller must or not be treated as subordinated to the interests and rights of private persons.

An example: The data subject purchases pizza on-line and gives his/her delivery address. The data subject in this case is the client of the pizza seller, who has a rightful interest in the processing of personal data (address) of the data subject in order to be able to perform the delivery, that is how the necessity requirement is fulfilled. Accordingly, this merchant must not add a checkbox to the payment process asking thereby consent to processing the data subject's data for the data subject may reasonably presume that upon the communication of the data they shall be processed. The pizza seller shall not however be entitled to treat this consent as given forever, and to sell it, for example to the neighbouring Chinese restaurant that the latter could send to the data subject publicity materials.

The General Data Protection Regulation gives also some more examples for rightful interests, such as the prevention of fraud, internet security or the sharing of information with the authorities regarding potential crimes even if the groups of related institutions "may have rightful interest" in sharing the personal data of clients and employees.

Rightful interest can be the most appropriate legal basis for processing the data of a private person, if:

- processing is not prescribed by law, but it offers an undisputable advantage for you or for others
- its impact on the private person's privacy is limited
- the private person can reasonably presume in which way your shall use his/her data
- you cannot or do not want to give the right of full control (i.e., the right of consent) to the private individual, or stalk him/her by annoying requests for consent in cases in which, by all probabilities, the private person shall raise no objection to the processing of his/her data.

In order to check the legitimacy of processing a rightful interest opinion can be made.

In the final analysis, the private person can object data processing on the grounds of rightful interest. If so, the data controller has the opportunity to defend himself. Even though the consent of the data subject has been given, he/she can revoke it at any time and ask for his/her data to be erased.

SPECIAL CATEGORIES OF PERSONAL DATA

The General Data Protection Regulation identifies the following special categories:

1. race and ethnicity
2. data concerning the private person's religious or philosophical beliefs
3. data on the private person's trade union membership
4. data on the private individual's sexual life and orientation
5. medical data
6. biometric identification data and DNA
7. data on convictions and criminal acts.

The General Data Protection Regulation tries to establish a balance between the purposes for which the organizations collect and use the personal data, and the right of private persons to privacy. Data falling within the above categories can be never made publicly accessible. When processing such data, the data controller shall pay utmost attention to their security and protection and secure the legal bases for their processing.
It is not recommended to collect and process data falling into the above categories, in general. If they still have to be, then the purposes of and legal basis for their collection and processing must be clearly recorded.

RIGHTS OF THE DATA SUBJECT

The main goal of the General Data Protection Regulation is to protect private individuals in all respects. In order to prevent unlawful processing of their data, it has vested the following rights in the data subject: the **right of being informed** on the processing of personal data.

- This right renders it possible for the data subject to ask from the Company information on what personal data of his/her are processed and for what purpose or goal? E.g., the client may ask for the list of the data processors with whom the Company shares the data subject's personal data.

The right of access to personal data

- This right makes it possible for the data subject to have access to his/her personal data being processed and, thus, inspect them and to get a copy of all his/her personal data concerned.

Right to rectification

- This right provides for the data subject the opportunity to ask for the amendment of his/her personal data if he/she is of the opinion that his/her personal data are not ready-to-date or accurate .

Right to erasure

- This right ensures for the data subject the opportunity to have his/her data deleted. As a rule, this applies to situations where the contact with the client/data subject has ceased. It is important, however, to note, that this is not an absolute right and is applied depending on whether the storage schedule and storage period are or not in compliance with the relevant statutory provisions.

Right to limit the scope of processing

- It allows the storage of data without processing. There are several possible scenarios: first and foremost, that the data subject thinks that his/her data are not correct and the data processor needs longer time to ascertain the accuracy of the data; on the second hand, if data processing is unlawful and instead of erasure the data subject recommends limitations and, on the third hand, if the data processor no more needs them for the achievement of his goals but keeps them for the event that legal claims may arise and, finally, if based on Section 21(1) the data subject protests against processing. In this case the data are used to ascertain, whether the rightful interest of the data processor takes or not precedence over the legal standing of the data subject.

Right of data transmission

- This right secures for the data subject the opportunity to ask for his/her data to be transmitted. As part of the relevant application the data subject may ask for returning to him/her his/her data or the transmission thereof to another data controller. The personal data so to be transmitted must be transmitted or handed over in machine readable electronic format.

Right to protest

- It is this right that secures for the data subject the opportunity to protest against the processing of his/her personal data. As a rule, this operates in the same way as the right to withdraw consent, when consent has been properly asked for and nothing else than legitimate data processing has taken place. On the other hand, in special cases the client can ask for his/her personal data not to be processed for certain purposes, e.g., if he/she has a pending lawsuit.

Right related to automated decision-making and profiling

- This right allows the data subject to protest against decisions relying on an automated processing of data. The right means that the client can ask for his/her application (e.g., a credit application) to be revised and assessed by a natural person if he/she is of the opinion that the automated processing of his/her application did not or would not take into account the specific situation he/she is in.

The application can be lodged by the individual or his/her legal representative. The individual making such appeal can be a client, employee, an employee elsewhere but working for the Company or a supplier. As a rule, applications of this type must be made in writing.

RIGHTS AND OBLIGATIONS OF DATA CONTROLLERS AND DATA PROCESSORS

The data controller:

- collects the personal data and has the relevant legal basis;
- decides which personal data must be collected;
- decides on t how to amend the data;
- determines the purpose or purposes of using the data;
- decides on whether the data can or not be shared and if yes, then with whom?;
- determines the length of the storage of the data.

The data processor appointed by the data controller can perform and execute the following tasks:

- can use IT systems or other methods for collecting personal data;
- uses certain means (tools) or techniques for collecting personal data;
- installs the security devices protecting personal data;
- stores personal data;
- transmits personal data between organizations;

OBLIGATIONS OF THE DATA CONTROLLER

The data controller shall implement proper **technical and organizational measures** and secure **compliance** with the applicable statutory provisions and, especially the
General Data Protection Regulation and provide for the certification thereof;
Duties of the data controller:
Implementation of the data protection **policies**;
Protection of data both during planning and implementation: the application of adequate methods of protection both during the planning of processing and the actual processing operations;
In case of data controllers from outside the EU, **appointment in writing of a representative seated in the member state,** where the controlled data subjects live obligatory;

1 except that processing is only occasional or the data controller is an authority or state organization

It is the data controller's responsibility to **employ employees who represent a substantial proof** for the implementation of proper technical and organizational measures;
The data controller shall conclude written contracts with the processor, that include the requirements set down in **Section 28 (3)** (e.g., that during the processing of personal data the data processor can act only based on and in conformity with the written instructions of the data controller, and that it is the data controller who shall decide whether the data processor should erase or return the data following the execution of the services, etc.);
The data controller shall keep written records of the processing activities. The records shall especially include what is prescribed by the provisions of Section 30 (1)2 and shall be placed at the disposal of the supervising authorities upon request. The data controller shall implement adequate **technical and organizational measures** to **secure the proper security** of data processing. Such measures may include pseudonymization/declaring confidential, maintaining secrecy, retrieval following physical/technical incidents;
The data controller shall secure that any **private person**, acting within his/her sphere of authority should process data solely and **exclusively if instructed to do so by the data controller;**
The data controller shall **inform** the **supervisory authorities** without undue delay but not later than 72 hours of any **infringement of personal data**. The data controller shall document every breach and also their impact and the measures taken to remedy them;
The data controller shall also immediately inform the data subjects of the breach of their personal rights, if the infringement in question may result in a grave violation of their rights and freedoms 3 ;
Before every data processing operation that entails potentially high risk the data processor shall carry out a **Data Protection Impact Assessment (DPIA)** and ask for the advice of the Data Protection Officer on it;
The data controller shall consult the supervising authorities before any such data processing that the **Data Protection Impact Assessment categorized as high risk**, if he failed to take any preliminary measures to mitigate the risks;
The data controller shall appoint a **Data Protection Officer,** whenever the appointment of such is mandatory under Section 37(1), publish of their data, and notify the supervising authority of the person of the data protection officer;
The data controller has to **involve the Data Protection Officer** in every issue touching the protection of personal data , support the Data Protection Officers, ensure the resources required for the discharge of their duties and ensure that the duties of the Data Protection Officer will not result in conflicts of interest.

2 cannot be employed where staff is below 250 (except that the rights of the data subjects can be breached or special data categories are processed (see section 9(1))
3 except that the terms and conditions laid down in Section 34 (3) materialize

OBLIGATIONS OF THE DATA PROCESSOR

Processing must comply with the requirements laid down in this Regulation.

- the data processor shall provide adequate guarantee for implementing the technical and organizational measures that ensure that data processing complies with the provisions of General Data Protection Regulation
- the data processor shall process the data according to the instructions of the data controller.

Limitations applicable to sub-contracting

- for the involvement of subcontractors in the data processing the preliminary written permit of the data controller is required
- the data controller shall be informed of the person of the data processor subcontractor so that the data controller would have enough time to protest

The data controller and the data processor shall **regulate their obligations in a contract.**

1. **Proving compliance:** records shall be kept of all the categories of data processing activities and should the data controller request that, compliance with the applicable data protection regulations be proved.
2. **Security:** application of appropriate safety measures to secure the protection of personal data.
3. **Notices of breaches:** The data controller must be notified without delay as soon as the data processor becomes aware of potential breaches.
4. 4.**Data Protection Officer:** it is mandatory to appoint data protection officer.
5. **Data transfer to third countries**: adequate protection for the data should be secured. Data transfer is allowed only on condition that the data subjects shall have executable rights as data subjects in the country where the data are transferred to.
6. **Code of Conduct:** the elaboration and implementation of a Code of Conduct whereby the safe and secure processing of data can be secured.

If any data controller participates in the processing of data, this data controller shall be liable for the damage caused by inadequate processing, unless he can prove that he is in no way responsible therefor. If there are several data controllers they are all jointly and severally liable for the damage and any of them can be compelled to provide efficient indemnification. The costs incurred shall afterwards be shared among the data controllers involved.

DATA PROTECTION IMPACT ASSESSMENT

Data Protection Impact Assessment shall be carried out if, by all probabilities, a specific type of data processing would entail too high a risk to the rights and freedoms of natural persons. The assessment shall be carried out still before data processing. The Data Protection Impact Assessment helps identifying possible problems still in an early phase, when they are more easy and less expensive to handle.
Especially, a Data Protection Impact Assessment is necessary in the following cases:

1. a systemic and extensive assessment of the personal standpoints of natural persons based on automated processing, including profiling, which shall by all probabilities serve as basis of decisions triggering legal consequences or other important impacts on natural persons
2. extensive processing of various types of special data or personal data related to criminal sentences and criminal acts
3. extensive systemic controlling of some publicly accessible area.

DATA PROTECTION OFFICER

A Data Protection Officer shall be appointed only at those data controllers and data processor whose activities consists of data processing operations that make the extensive systemic regular checking of data subjects necessary with regard to their special data, convictions or crimes. It is important to note that the Data Protection Officer

- is appointed based on his/her vocational skills and especially the expert knowledge of data protection law and practice
- may be an employee or an external services provider
- must furnish access data
- must be given adequate resources for the execution of his tasks and furthering his/her vocational skills
- reports to the top management and
- cannot be involved in any task as may cause a conflict of interests.

CONCLUSIONS

The General Data Protection Regulation emphasizes those requirements that have already existed in the various directives or other applicable statutory provisions. It focuses on the rights of data subjects and establishes the legitimate basis for data processing. Data subjects must receive detailed information and must give their consents to the processing of their data from their own wills. The data subjects cannot have less advantages than those who are willing to share more personal data than necessary or required. On the other hand the General Data Protection Regulation emphasizes the security of data processing and the provability of compliance, therefore, during their activities, data processors must use proper care for securing the protection of the privacy and data of the data subjects.