



**AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE
A PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

GUIDELINES Q&A WITH REFERENCE TO THE APPLICATION OF REGULATION (EU) 2016/679



romania2019.eu
Președinția României la Consiliul Uniunii Europene





Guidelines Q&A with reference to the application of Regulation (EU) 2016/679

1. What is the material scope of Regulation (UE) 2016/679?

Regulation (EU) 2016/679 applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system. Regulation (EU) 2016/679 applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

The Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- the monitoring of their behaviour as far as their behaviour takes place within the Union.

(Article 2 and Article 3 of the GDPR)

2. When the Regulation (EU) 2016/679 does not apply?

Regulation (UE) 2016/679 **does not apply** to the processing of personal data:

- in the course of an activity which falls outside the scope of Union law;
- by the Member States when carrying out activities related to external policy and the common security of the Union;
- by a natural person in the course of a purely personal or household activity;
- by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; these are regulated by the **Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of

criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA which was transposed by Law no. 363/2018 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, educative and safety measures and on the free movement of such data.

(Article 2 of the GDPR)

3. Regulation (EU) 2016/679 applies to the processing performed by natural persons for personal activity?

The General Data Protection Regulation (GDPR) **does not apply** to the processing by a **natural person in the course of a purely personal or household activity**.

Recital (18) of the GDPR states that the purely personal or household activity and thus with no connection to a professional or commercial activity should not have a connection to a professional or commercial activity. Personal or household activities could include *correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities*.

(Article 2 of the GDPR)

4. Regulation (EU) 2016/679 applies to the processing carried out by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, educative and safety measures and on the free movement of such data?

The General Data Protection Regulation does not apply to processing carried out by the competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, educative and safety measures and on the free movement of such data.

These processing are regulated by Law no. 363/2018 on the protection of natural persons with regard to the processing of personal data by competent

authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, educative and safety measures and on the free movement of such data, legal act that **transposed Directive (EU) 2016/680** of the European Parliament and of the Council of 27 April 2016.

The processing of personal data for carrying out the activities of maintaining and ensuring public order and safety **is performed only if they are provided by law and are necessary to prevent at least a danger to the life, the body's integrity or the health of a person or his/her property, as well as to fight crime.**

Law no. 363/2018 **does not apply** to the processing of personal data performed for carrying out activities in the field of national defence and national security, within the limits and with the restrictions established by the legislation in this field.

(Article 2 of the GDPR)

5. What does it mean controller?

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, ***the controller or the specific criteria for its nomination may be provided for by Union or Member State law.***

(Article 4 of the GDPR)

6. What does it means joint controllers?

Joint controllers are two or more controllers that jointly determine the purposes and means of processing.

They shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the Regulation, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the controllers are determined by Union or Member State law

to which the controllers are subject.

(Article 26 of the GDPR)

7. What does it mean processor?

Processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

The processing performed by a processor is regulated by Article 28 of the GDPR.

(Article 4 and Article 28 of the GDPR)

8. Is it necessary to notify the data processing to the National Supervisory Authority?

Taking into account that starting with the 25th of May 2018 the Regulation (EU) 2016/679 became applicable, the controllers no longer have the obligation to notify the data processing.

Therefore, the *On-line register for the evidence of the data processing* is no longer available on the website of the supervisory authority. Also, it is no longer necessary to use the notification number granted under Law no. 677/2001.

9. What obligations do I have as a data controller according to the Regulation (EU) 2016/679?

The obligations that the controller have are regulated by Chapter IV of the Regulation (EU) 2016/679.

Among the main obligations of the controller in applying the Regulation are:

- respecting the principles relating to processing of personal data (Article 5 of the Regulation);
- respecting the rights of the natural persons (Articles 12 to 23 of the Regulation);
- ensuring the security of the data (Article 25 and Article 32 of the Regulation);
- designating the data protection officer (Article 37 to 39 of the Regulation), as the case may be;

- notifying the personal data breaches (Article 33 of the Regulation), as the case may be;
- data protection impact assessment and respecting the rights of the natural persons (Article 35 of the Regulation), as the case may be;
- data processing mapping (Article 30 of the Regulation).

For additional information you can access the *Indicative guidelines for the application of the General Data Protection Regulation intended for the controllers* issued by the National Supervisory Authority.

The following guidelines issued by the European Data Protection Board can also be accessed:

- *Guidelines on the Data Protection Officer;*
- *Guidelines on the impact assessment;*
- *Guidelines on the notification of the personal data breaches;*
- *Guidelines on the right to data portability;*
- *Guidelines on the individual automated decisions and profiling;*
- *Guidelines on transparency;*
- *Guidelines on consent.*

10. What obligations do I have as a processor?

Where the processing is to be carried out on behalf of controller, it shall use only processors that provide sufficient guarantees for the implementation of appropriate technical and organisational measures, so that the processing complies with the requirements of the Regulation and ensures the protection of rights. the data subject (Article 28 of the Regulation).

The processing performed by a processor on behalf of a controller is governed by a contract or another legal act under Union or Member State law that is binding on the processor and set out *the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and right of the controller.*

(Article 28 of the GDPR)

11. What should be stipulated in the contract or the legal act concluded between the controller and the processor?

That contract or other legal act shall stipulate, in particular, that the processor:

- processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject;
- ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- adopts appropriate technical and organisational measures;
- respects the conditions for engaging another processor;
- 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;
- assists the controller in ensuring compliance with the obligations pursuant to the Regulation;
- 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 unless Union or Member State law requires storage of the personal data;
- makes available to the controller all information necessary to demonstrate compliance with its obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

(Article 28 of the GDPR)

12. When do I designate a representative of the controller or of the processor?

The controller or processor that is not established in the European Union has the obligation to designate a representative in the Union when it processes personal data belonging to data subjects established in the Union for activities related to:

- ***the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or***
- ***the monitoring of their behaviour as far as their behaviour takes place within the Union (Article 27 of the Regulation).***

(Article 27 of the GDPR)

13. When do I have to designate a data protection officer (DPO)?

The designation of a data protection officer is mandatory when:

- the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- the public authority and bodies are: *Chamber of Deputies and Senate, Presidential Administration, Government, the ministries, the other specialised bodies of the central public administration, the autonomous public authorities and institutions, the local public administration authorities and at county level, other public authorities, as well as the subordinated/under coordination institutions; also, the clubs and associations and public utility foundations are assimilated to public authorities/bodies* – Article 2 paragraph (1) letter a) of the Law no. 190/2018;
- 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
- the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences (Article 37 paragraph (1) of the Regulation);
- in cases other than the ones mentioned above, the controller or the processor or the associations and other bodies representing categories of controller or processors may designate or, where required by Union law or national law, appoint a data protection officer. The data protection officer may act in favour of such associations and other bodies representing controllers or processors.

For more information you can access the *Guidelines on the data protection officer* issued by the European Data Protection Board.

(Article 37 of the GDPR)

14. What does it mean processing on a large scale?

When determining whether the processing is on a large scale, the following factors should be considered:

- **the number of the data subjects** (either an exact number or a percentage of the relevant population);
- **the volume of data** and/or the range of different elements of data being processed;
- the **duration** or permanence of the data processing activity;

- the geographical **surface** of the processing activity.

For additional information, you can consult the *Guidelines on the Data Protection Officer* issued by the European Data Protection Board.

15. What conditions the data protection officer should fulfil?

The data protection officer is designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil its tasks.

For additional information, you can consult the *Guidelines on the Data Protection Officer* issued by the European Data Protection Board.

(Article 37 din RGPD)

16. Is it allowed to appoint a single data protection officer for a group of undertakings or for several public authorities and bodies?

A group of undertakings can appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

The notion of accessibility refers to the tasks of the data protection officer as a point of contact regarding the data subjects, the supervisory authority, but also internally within the organisation.

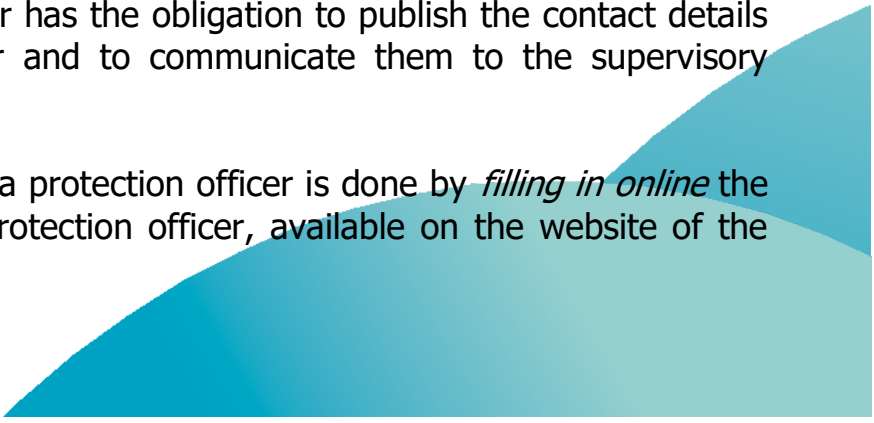
Also, *several public authorities or bodies* can designate a single data protection officer, by taking account of their organisational structure and size.

For additional information, you can consult the *Guidelines on the Data Protection Officer* issued by the European Data Protection Board.

17. How shall I communicate the data protection officer to the supervisory authority?

The controller or the processor has the obligation to publish the contact details of the data protection officer and to communicate them to the supervisory authority.

The communication of the data protection officer is done by *filling in online* the form for declaring the data protection officer, available on the website of the



authority www.dataprotection.ro, under Section "Data Protection Officer", followed by clicking the button "Trimite chestionarul" (Send the questionnaire).

Where a *group of undertakings or several public authorities or bodies* appoint a single data protection officer, each data controller or processor shall fill in the form for declaring the data protection officer available on the website of the authority, under Section "Data Protection Officer".

18. How can I amend the details of the data protection officer from the on-line form submitted to the supervisory authority?

In the event of changes/completions regarding the information contained in the declaration form of the data protection officer, it is necessary to complete and transmit to the supervisory authority a new form in the same way as described in point 17.

19. What are the legal conditions for processing the personal data, other than the special ones?

Processing shall be lawful only if and to the extent that at least one of the following conditions provided by paragraph (1) applies:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- processing is necessary for compliance with a legal obligation to which the controller is subject;
- processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular

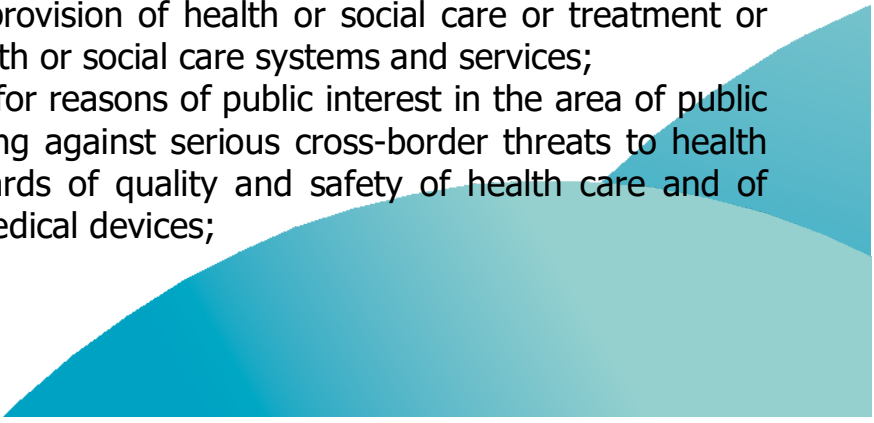
where the data subject is a child (is not applicable to processing carried out by public authorities in the performance of their tasks).

(Article 6 of the GDPR)

20. What are the conditions for processing the special categories of personal data?

Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

The processing of these categories of data is allowed only in the following conditions:

- ✓ the data subject has given explicit consent to the processing of those personal data for one or more specified purposes;
 - ✓ processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law;
 - ✓ processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
 - ✓ processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim;
 - ✓ processing relates to personal data which are manifestly made public by the data subject;
 - ✓ processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
 - ✓ processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law;
 - ✓ processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services;
 - ✓ processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices;
- 

- ✓ processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The processing of genetic data, of biometric data or of health data for the purpose of automated decision-making or profiling is permitted with the explicit consent of the data subject or if the processing is carried out under explicit legal provisions, with appropriate measures protecting the rights, freedoms and legitimate interests of the data subject.

(Article 9 of the GDPR and Article 3 of the Law no. 190/2018)

21. What are the conditions for granting and validity of the consent?

The consent of the data subject must be granted through an unequivocal action that constitutes a freely expressed, specific, informed and clear manifestation of the agreement of the data subject for the processing of his/her personal data, such as:

- written declaration in an intelligible and easily accessible form, using clear and plain language;
- electronic declaration – ticking a box when the persons visits a website;
- statement verbally expressed.

The absence of a reply, the boxes checked in advance or the absence of an action does not constitute consent.

The consent should cover all the processing activities carried out for the same purpose or for the same purposes. If data processing is done for more than one purpose, consent should be given for all the purposes of processing.

The controller shall be able to demonstrate that the data subject has consented to the processing of his/her personal data.

When **assessing whether consent is freely given**, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

For additional information, please consult the *Guidelines on consent* issued by the European Data Protection Board.

22. If the processing of data other than those of a special nature is

necessary in order to fulfil a legal obligation incumbent upon me as a controller, it is still necessary to obtain the consent of the data subjects?

When the processing is necessary in order to fulfil a legal obligation of the controller, it is no longer necessary to obtain the consent of the data subjects (for example, processing the data of the employees by the employer in order to transmit them to REVISAL).

For additional information, please consult the *Guidelines on consent* issued by the European Data Protection Board.

23. What are the conditions for the withdrawal of the consent?

The withdrawal of the consent should be done by respecting certain conditions such as:

The data subject shall have the right to withdraw his/her consent at any time and as easy as he/she granted the consent;

The data subject should be able to withdraw his/her consent without any prejudices; The controller should make it possible to withdraw the consent free of charge or without diminishing the quality of the service;

Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

In the case of withdrawal of consent, all the data processing operations that were based on the respective consent and took place before its withdrawal and in accordance with Regulation (EU) 2016/679, *continue to be legal*, but the controller should cease the actions of the processing concerned. If there is no other legal basis to justify the processing of data, they should be deleted by the controller.

For additional information, please consult the *Guidelines on consent* issued by the European Data Protection Board.

(Article 7 of the GDPR)

24. Under what conditions the personal data of the children may be processed in relation to the offer of information society services?

The processing of the personal data of a child, based on the **consent**, shall be lawful where the child is **at least 16 years old**.

Where the child is **below the age of 16 years**, such processing shall be lawful only if and to the extent that **consent is given or authorised by the holder of parental responsibility** over the child.

The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology (Article 8 of Regulation (EU) 2016/679).

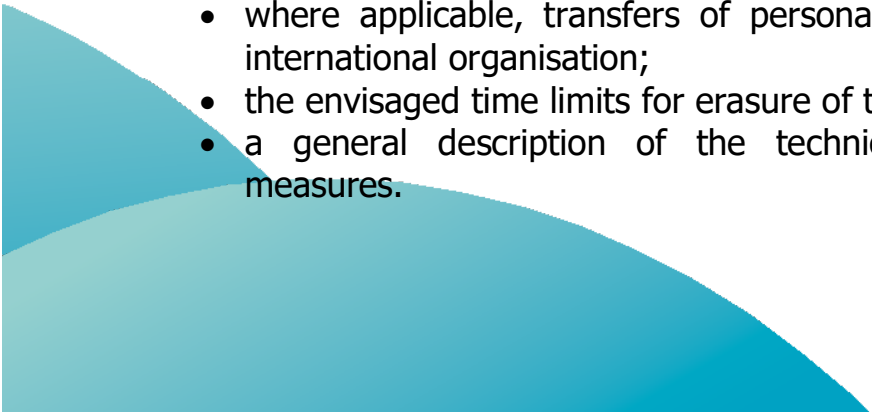
For additional information, please consult the *Guidelines on consent* issued by the European Data Protection Board.

(Article 8 of the GDPR)

25. Are the controllers or the processors required to maintain a record of data processing?

Each controller and each processor shall maintain a record of processing activities under its responsibility in writing, including in electronic form.

The record of the processing shall contain all the following information:

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

The exceptional situations provided by Article 30 paragraph (5) of Regulation (EU) 2016/679 are of strict interpretation.

(Article 30 of the GDPR)

26. When is it necessary to perform a data protection impact assessment?

The data protection impact assessment by data controllers shall be mandatory especially in the following cases:

1. the processing of personal data in order to perform a 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;
2. b) processing on a large scale of special categories of data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation or of personal data relating to criminal convictions and offences;
3. c) the processing of personal data having as purpose the systematic monitoring of a publicly accessible area on a large scale, such as: video surveillance in shopping centres, stadiums, markets, parks or other such spaces;
4. d) processing on a large scale of personal data of vulnerable persons, especially children and employees, through automatic means of systematic monitoring and/or recording of behaviour, including in order to carry out advertising, marketing and publicity activities;
5. e) processing on a large scale of personal data through the innovative use or the implementation of new technologies, especially if the respective operations limit the ability of the data subjects to exercise their rights, such as the use of facial recognition techniques to facilitate access to different spaces;
6. f) processing on a large scale of data generated by devices with sensors that transmit data over the Internet or other means ("IoT" applications, such as smart TVs, connected vehicles, smart meters, smart toys, smart cities or other such applications);
7. g) processing on a large scale and/or systematic of traffic and/or location data of natural persons (such as Wi-Fi monitoring, processing of geo-

location data of passengers in public transport or other such situations) when processing is not necessary to provide a service requested by the data subject.

(Decision of the president of the supervisory authority no 174/2018)

For additional information, on the website of the supervisory authority www.dataprotectio.ro you can consult:

- the *Guidelines on the data protection impact assessment* issued by the European Data Protection Board, as well as
- the *Decision of the president of the supervisory authority no. 174/2018 on the list of kind of processing operations which are subject to the requirement for a data protection impact assessment.*

27. What should the data protection impact assessment contain?

The assessment shall contain at least:

- a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and
- 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 this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

For additional information, you can consult the *Guidelines on the data protection impact assessment* issued by the European Data Protection Board, as well as the *Indicative Guidelines for the application of the General Data Protection Regulation* issued by the National Supervisory Authority.

28. It is necessary to submit the data protection impact assessment for the approval by the supervisory authority?

The controller shall consult the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the

risk.

Such a risk is likely to be generated by certain types of processing, as well as by the magnitude and frequency of the processing, which may also lead to injury or may affect the rights and freedoms of natural persons.

The impact assessment shall be submitted at the request of the National Supervisory Authority in the course of conducting an investigation.

29. When should a data protection impact assessment be carried out?

The data protection impact assessment should be carried out before starting the processing.

The data protection impact assessment should start as soon as possible in the elaboration of the processing operation, even if some of the processing operations are not yet known.

The data protection impact assessment is an ongoing process, especially if a processing operation is dynamic and constantly changing.

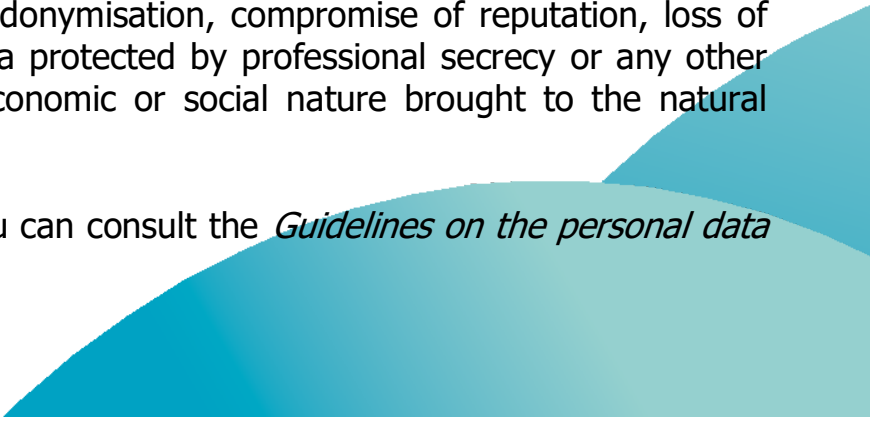
For additional information, you can consult the *Guidelines on the data protection impact assessment* issued by the European Data Protection Board.

30. What does it mean personal data breach?

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

The personal data breach may lead to physical, material or moral damages to natural persons, such as the loss of control over their personal data or the limitation of their rights, discrimination, theft or identity fraud, financial loss, unauthorised reversal of pseudonymisation, compromise of reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant disadvantage of economic or social nature brought to the natural person concerned.

For additional information, you can consult the *Guidelines on the personal data*



breach notification issued by the European Data Protection Board.

(Article 4 of the GDPR)

31. What is the deadline for the notification of the personal data breaches?

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 competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

(Article 33 of the GDPR)

32. Which is the way to notify the personal data breach?

In case of a personal data breach, it is necessary to fill in the on-line the form adopted by Decision no. 128/2018 of the president of the Supervisory Authority for the notification of the personal data breach in accordance with Regulation (EU) 2016/679, available on the website of the supervisory authority www.dataprotection.ro.

The notification form in pdf. format, editable, is filled in by the controllers, signed digitally and transmitted to the e-mail address of the supervisory authority, brese@dataprotection.ro. The forms that will not be digitally signed shall not be taken into consideration.

The controller should keep the documents regarding all cases of personal data breach, including a description of the factual situation in which the personal data breach, its effects and remedial measures took place.

Information about the method of notification are available on the website of the supervisory authority, www.dataprotection.ro, under section "GDPR data breach", as well as in the *Guidelines on the personal data breach notification* issued by the European Data Protection Board.

33. What are the rights of the data subject?

Chapter III of Regulation (EU) 2016/679 regulates the rights of the data subjects:

- right to information (Articles 13 and 14);
- right of access (Article 15);
- right to rectification (Article 16);
- right to erasure ("right to be forgotten" – Article 17);
- right to restriction of processing (Article 18);
- right to data portability (Article 20);
- right to object (Article 21);
- right not to be subject to a decision based solely on automated processing (Article 22);
- right to submit a complaint to a supervisory authority (Article 77).

In order to exercise the rights provided by Articles 15 to 22 of Regulation (EU) 2016/679, the data subjects shall submit a request to the controller in this regard.

For additional information, you can consult the *Guidelines on the right to data portability*, the *Guideline on automated individual decisions and profiling*, the *Guidelines on transparency* adopted by the European Data Protection Board.

34. What is the timeframe the controller should respond to a request to exercise the rights of the data subject?

The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

(Article 12 of the GDPR)

35. What information the controller should provide to the data subject must provide?

The controller shall provide the data subject with the following information, when the data is obtained directly or indirectly from the data subject:

1. the identity and the contact details of the controller and, where applicable, of the controller's representative;
2. the contact details of the data protection officer, where applicable;

3. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
4. the categories of personal data concerned (where the data were obtained indirectly);
5. the legitimate interests pursued by the controller or by a third party (where applicable);
6. the recipients or categories of recipients of the personal data;
7. the intention of the controller to transfer personal data to a third country or international organisation and the conditions for performing the transfer (where applicable);
8. the period for which the personal data will be stored (or the criteria used to determine that period);
9. the existence of the rights of the data subjects provided by the Regulation;
10. the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
11. the right to lodge a complaint with a supervisory authority;
12. 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;
13. the existence of automated decision-making, including profiling, information about the logic involved and the consequences of such processing for the data subject;
14. the processing of personal data for a purpose other than that for which the personal data were collected (where applicable);
15. from which source the personal data originate and whether it came from publicly accessible sources (for data obtained indirectly).

(Articles 13 and 14 of the GDPR)

36. When is it necessary to inform the data subjects in case the personal data were not obtained from them?

Where the personal data were not obtained directly from the data subject, the controller shall inform the data subject:

1. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

2. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or
3. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

With reference to the method used for informing the data subjects (regardless of the legal ground of the processing, consent or based on the exceptions), the controller shall take appropriate measures, depending on the circumstances of the data processing, to provide to the data subject the information provided by the GDPR in a **concise, transparent, intelligible and easily accessible form**, using **clear and plain language**.

The information is provided **in writing or by other means**, including, when appropriate, in **electronic format**.

For information a generic information can be used, displayed on the controller's website, displayed on the notice board at the controller's office, direct information notes of the data subject, concurrently with the provision of brochures and leaflets, as well as other modalities that are set by the controller.

For additional information, you can consult the *Guidelines on transparency* issued by the European Data Protection Board.

(Article 14 of the GDPR)

37. The data subject can have access to his/her personal data processed by the controller?

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed. Where that is the case, the data subject has the right to know and to being communicated the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipient or categories of recipient to whom the personal data have been or will be disclosed;
- the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with a supervisory authority;
- any available information as to their source (for data obtained indirectly);

- the existence of automated decision-making, including profiling, information about the logic involved and the consequences of the processing for the data subject
- the transfer to a third country or to an international organisation and the adequate safeguard regarding the transfer.

The controller shall provide the data subject with a copy of the personal data undergoing processing. For any other copies requested by the data subject, the controller may charge a reasonable fee taking into account the administrative costs.

If the data subject submits the request in electronic format and does not choose to receive the information in another format, the answer is provided in an electronic format currently used.

For additional information, you can consult the *Guidelines on transparency* issued by the European Data Protection Board.

(Article 15 of the GDPR)

38. What are the situations in which the data subject may obtain the erasure of the personal data by the controller (“the right to be forgotten”)?

The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to the conditions for exercising the right to object;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services to a child.

Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking into account of available technology

and the cost of implementation, shall take reasonable measures (including technical ones), to inform the other controllers that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

(Article 17 of the GDPR)

39. What are the conditions for exercising the right to object?

The data subjects shall have the right to object, on grounds relating to his/her particular situation, to processing of personal data concerning him/her when data are processed for:

- ❖ performing a task carried out in a public interest
- ❖ performing a task carried out in the exercise of official authority vested in the controller
- ❖ the purposes of the legitimate interests pursued by a controller or by a third party
- ❖ scientific or historical research purposes or statistical purposes, except the case where the processing is necessary for the performance of a task carried in a public interest.

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing. In this case, the controller shall no longer process personal data.

At the latest at the time of the first communication with the data subject, the right to object shall be **explicitly** to the attention of the data subject and shall be presented **clearly and separately** from any other information.

(Article 21 of the GDPR)

40. What are the situations in which the data subject cannot obtain the erasure of the personal data from the controller?

The data subject cannot obtain the erasure of the personal data from the controller to the extent that the processing is necessary:

- ❖ for exercising the right of freedom of expression and information;
- ❖ for compliance with a legal obligation;
- ❖ for reasons of public interest in the area of public health;
- ❖ for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (in so far as the right is likely to render impossible or seriously impair the achievement of the objectives of that processing);
- ❖ for the establishment, exercise or defence of legal claims.

(Article 17 of the GDPR)

41. What are the conditions in which the data subject can transmit his/her personal data to another controller (right to data portability)?

The data subject shall have the right to receive the personal data concerning him/her, which he/she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

- the processing is based on **consent** and
- the processing is carried out by **automated means**

The data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

The right shall not adversely affect the right to obtain the erasure of the data and shall not adversely affect the rights and freedoms of others.

(Article 20 of the GDPR)

42. In what situations the data subject can be subject to a automated individual decision, including profiling?

The rule is that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him/her or similarly significantly affects him/her.

However, the data subject may be the subject to a decision based on automatic

processing, including profiling, if the decision:

- is **authorised by Union or Member State law** to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests
- is necessary for **entering into, or performance of, a contract** between the data subject and a data controller or
- is based on the data subject's explicit **consent**.

In the latter two cases the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests concerning at least:

- the right to obtain the human intervention on the part of the controller,
- to express his/her point of view and
- to contest the decision.

The decision shall not be based on special categories of personal data, unless the data is processed based on the consent or for substantial public interest and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

(Article 22 of the GDPR)

43. How data transfer to a third country or international organisation is carried out?

The basic principle of transfers is that any personal data can be transferred only if the conditions set out in the Regulation are met by both the controller and the processor, including in respect of onward transfers in other third countries.

The transfer of personal data can be done through:

- the adequate decisions adopted by the European Commission concerning the level of protection ensured by a third country;
- standard contractual clauses adopted by the Commission;
- binding corporate rules in accordance with Article 47 of the Regulation;
- other modalities provided in by Article 46 and Article 49 of the Regulation such as:
 - a legally binding and enforceable instrument between public authorities or bodies;
 - standard data protection clauses adopted by a supervisory authority and approved by the European Commission;

- an approved code of conduct together with binding and enforcement commitments of the controller or processor in the third country;
- an approved certification mechanism together with binding and enforcement commitments of the controller or processor in the third country;
- contractual clauses between the controller or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or
- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

Derogations for specific situations (Article 49 of the GDPR)

In the absence of an adequacy decision or of appropriate safeguards, the transfers may take place only on one of the following conditions:

- the explicit consent of the data subject – prior information
- the performance of a contract between the data subject and the controller (pre-contractual measures)
- the conclusion/performance of a contract concluded in the interest of the data subject
- public interest
- establishment, exercise or defence of legal claims
- the protection of the vital interests of the data subject or of other persons
- providing of information from a register which is publicly accessible
- other situations, in certain conditions, by presenting certain appropriate safeguards by the controller.

For additional information, you can consult the following documents, available on the website of the supervisory authority www.dataprotection.ro:

- *Guidelines on derogations applicable to international transfers (Article 49 of the General Data Protection Regulation)*, issued by the European Data Protection Board;
- *Recommendation on the approval of the Controller Binding Corporate Rules form for the personal data transfer (WP 264)*;
- *Working Document on the approval procedure of the binding corporate rules for controllers and processors, according to the GDPR (WP 263)*;
- *Working Document establishing a table with the elements and principles to be found in the binding corporate rules (WP 256)*;

- *Working Document establishing a table with the elements and principles to be found in the binding corporate rules applicable to processors (WP 257);*
- *Recommendation on the approval of the Processor Binding Corporate Rules form for the personal data transfer applicable to processors (WP 265).*

44. What are the situations in which the supervisory authority issues authorisations for the transfer of personal data?

Where the transfer cannot be performed based on an adequate decision, the controller or processor may transfer personal data to a third country or international organisation, subject to the authorisation from the supervisory authority, by:

- contractual clauses between the controller or processor and controller, processor or the recipient of the personal data in the third country or international organisation; or
- provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

For additional information you can consult *Opinion no. 4/2019 on the administrative arrangements for the transfer of personal data between the financial supervision authorities from the EEA and the financial supervision authorities outside the EEA*.

(Article 46 paragraph (3) of the GDPR)

45. The decisions adopted by the European Commission on the basis of Article 26 paragraph (4) of Directive 95/46/EC are still valid after the application of Regulation (EU) 2016/679?

The decisions adopted by the European Commission on the basis of Article 26 paragraph (4) of Directive 95/46/EC **shall remain in force until amended, replaced or repealed by a Commission decision** adopted in accordance with paragraph (2) of Article 46 of Regulation (EU) 2016/679

As such, the following decisions are applicable:

- Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third

countries under Directive 95/46/EC of the European Parliament and of the Council;

- Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries;
- Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC.

46. What measures should the controllers and processors take in order to ensure the security of the processing of personal data?

In order to ensure a level of security appropriate, the controllers and processors shall implement appropriate technical and organisational measures such as:

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing;
- the pseudonymisation and encryption of personal data, as the case may be (the implementation of the pseudonymisation of the personal data may reduce the risks for the data subjects and may help the controllers and processors to fulfil the data protection obligation);
- ensuring that any natural person acting under the authority of the controller or of the processor who has access to personal data does not process them, unless he/she is required to do so by Union or Member State law.

Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which the controller or processor demonstrates compliance with the requirements concerning the implementation of adequate technical and organisational measures.

(Article 32 of the GDPR)

47. What does it mean “pseudonymisation”?

Pseudonymisation is defined as the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

(Article 4 of the GDPR)

48. How long can I store the personal data?

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, which the implementation of certain safeguards.

Thus, the controller has the possibility to have different retention periods of the data, depending of the purpose/purposes of the processing and for the period necessary for their achievement, either by establishing from its own initiative of a maximum period of retention, by respecting the proportionality principle, or by respecting some periods provided by different specific legal acts.

If the storage period is established by legal acts that regulate specific activity domains, to the extent that is imposed, the authorised entities should amend/supplement them so that the rules are in accordance with the General Data Protection Regulation

(Article 5 of the GDPR)

49. The owners’ associations can process the personal data of the owners/tenants by using the means of video surveillance based on their legitimate interest?



The processing of personal data through the use of **closed-circuit television** systems with the possibility of recording and storing images and data is subject both to the provisions of the General Data Protection **Regulation** and **Law no. 333/2003** regarding the protection of the objectives, assets, values and protection of persons, amended and supplemented, and of the Methodological Norms for applying this law.

In the context in which the installation of a video surveillance system is necessary in order to achieve a legitimate interest of the owners' association (ensuring the security and protection of persons, goods and values, buildings and public utility installations, as well as the surrounding areas), the decision to install such a system must be adopted at the general meeting of the owners' association.

According to Article 48 paragraph (1) of **Law no. 196/2018 on the establishment, organisation and functioning of owners' associations and the administration of condominiums**, "The General Assembly may take decisions, if the majority of the owners members of the owners' association are personally present or through representatives who have a written and signed empowerment by the owners on whose behalf they are voting". Also, paragraph (3) of the same article specifies that the decisions of the general meeting of the owners' association can be adopted by the vote of the majority of them.

In addition, the interests, rights and freedoms of the data subjects should be taken into account. They should be informed in advance about taking such a measure. In this regard, a suitable icon should be installed in the monitored spaces, containing a representative image, positioned at a reasonable distance from the places where the surveillance equipment is located, so that it can be seen by any person.

The National Supervisory Authority recommends that the period of retention of personal data (images) processed by the association as a result of the installation of the video surveillance system should not exceed 30 days.

Exceptions may be made in justified cases, in which events have occurred, that require the storage of only relevant images for a longer period of time necessary for the fulfilment of the respective purposes (e.g. until the final resolution of a criminal case by the judicial bodies).

50. Under what conditions the owners' associations can publish the

payment?

In accordance with Article 6 of Regulation (EU) 2016/679, the processing shall be lawful only if and to the extent that at least one of the conditions stipulated in paragraph (1) of the same article applies.

Regulation (EU) 2016/679 introduces in Article 5 a new principle relating to processing of personal data, accountability principle, according to which the controllers shall be responsible for, and be able to demonstrate compliance with all the principles relating to processing of personal data ("lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation", as well as "integrity and confidentiality").

Pursuant to Article 5 of the Regulation, personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

The processing of data belonging to owners within the context of publishing the payments lists can be carried out with their consent based on the provisions of Article 6 paragraph (1) letter a) of the Regulation, in compliance with the principles and rules for the protection of data established by this legal act.

51. Public institutions may publish on their own website the personal data of the persons participating in competitions for the filling in of positions corresponding to the contractual functions?

Pursuant to Article 6 of Regulation (EU) 2016/679, the processing shall be lawful only if and to the extent that at least one of the conditions stipulated in paragraph (1) of the same article applies, some of them being the consent of the data subjects or compliance with a legal obligation.

Therefore, if the legal provisions in this matter do not expressly provide as legal obligation the publication on the website of the public authorities of the name and surname of the candidates, this can be done only with the consent of the candidates, based on the provisions of Article 6 paragraph (1) letter a) of the Regulation, in compliance with the principles and rules of data protection established by this normative act.

52. Who can draw up codes of conducts?

According to the provisions of Article 40 paragraph (2) of Regulation (EU)

2016/679, associations and other bodies representing categories of controllers or processors may prepare codes of conduct, amend or extend such codes, for the purpose of specifying the application of the Regulation.

For additional information you can consult *Guidelines 1/2019 on the codes of conducts and the monitoring bodies under Regulation (EU) 2016/679* issued by the European Data Protection Board.

53. The codes of conduct are submitted for opinion and approval to the supervisory authority?

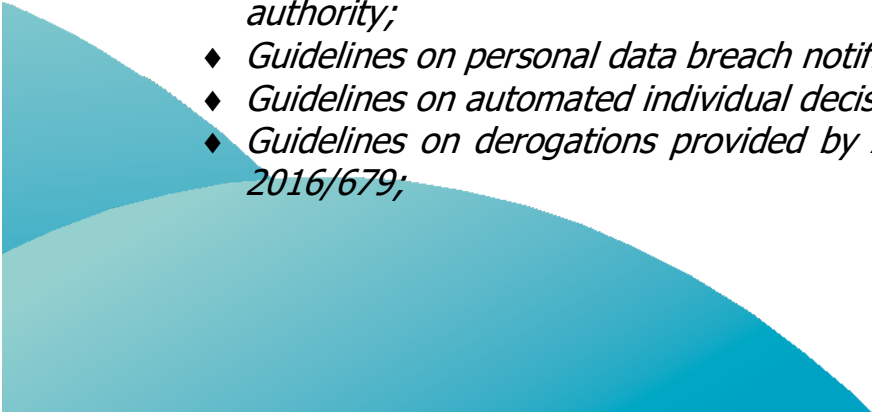
Associations and other bodies representing categories of controllers or processors which intend to prepare a code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with the Regulation and shall approved that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards.

For additional information you can consult *Guidelines 1/2019 on the codes of conducts and the monitoring bodies under Regulation (EU) 2016/679* issued by the European Data Protection Board.

(Article 40 of the GDPR)

54. What guidelines did the European Data Protection Board issued?

The European Data Protection Board adopted and published a series of useful guidelines and opinions for the interested parties such as:

- ◆ *Guidelines on data protection officers;*
 - ◆ *Guidelines on consent;*
 - ◆ *Guidelines on the right to data portability;*
 - ◆ *Guidelines on transparency;*
 - ◆ *Guidelines on the data protection impact assessment;*
 - ◆ *Guidelines identifying a controller or processor's lead supervisory authority;*
 - ◆ *Guidelines on personal data breach notification;*
 - ◆ *Guidelines on automated individual decision-making and profiling;*
 - ◆ *Guidelines on derogations provided by Article 49 of the Regulation (EU) 2016/679;*
- 

- ◆ *Guidelines 4/20018 on the accreditation of the certification bodies under Article 43 of the Regulation (EU) 2016/679;*
- ◆ *Guidelines 1/2018 on certification and identification of certification criteria pursuant to Articles 42 and 43 of the Regulation (EU) 2016/679;*
- ◆ *Guidelines on the application and establishing the administrative fines pursuant to the Regulation (EU) 2016/679;*
- ◆ *Guidelines 1/2019 on the codes of conduct and the monitoring bodies pursuant to the Regulation (EU) 2016/679;*
- ◆ *Position document on the derogations from the obligation to maintain a record of the processing activities pursuant to Article 30 paragraph (5) of the Regulation (EU) 2016/679;*
- ◆ *Opinion 4/2019 on the administrative arrangements for the transfer of personal data between the financial supervision authorities from the EEA and the financial supervision authorities outside the EEA.*

These guidelines are accessible on the website of the authority, www.dataprotection.ro, under the section dedicated to the new General Data Protection Regulation, as well as on the website of the European Data Protection Board www.edpb.europa.eu.

55. What guidelines did the National Supervisory Authority issued?

The National Supervisory Authority made available on its website:

- ◆ the *Indicative Guidelines for the application of the General Data Protection Regulation* and
- ◆ the *Guidelines Q&A with reference to the application of the Regulation (EU) 2016/679*, available on the website of the national supervisory authority, under Section dedicated to the General Data Protection Regulation.

56. What are the novelties brought by Law no. 190/2018?

Law no. 190/018 brings the following elements of novelties:

- **expressly mentions the public authorities and bodies** to which the provisions of the General Data Protection Regulation apply;
- **defines a series of terms** such as: national identification number, remedial plan, remedial measure, remedial deadline (Article 2);
- **establishes special rules for the processing of certain categories of personal data**, such as genetic data, biometric data or data concerning health (Article 3);

- **establishes the conditions for the processing of a national identification number** (e.g. personal identification number) when the processing is necessary for the legitimate interests pursued by the controller or a third party (Article 4);
- **sets out specific provisions for the processing of personal data in the context of employment** (Article 5);
- **provides derogations** for the processing of personal data for journalistic purposes or the purposes of academic, artistic or literary expression or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (Article 7 and Article 8);
- **mentions the conditions of the designation and the tasks of the data protection officer**, especially in the case of public authorities/institutions and public bodies (Article 10);
- **designates the Romanian Accreditation Association – RENAR** as the national accreditation body for the certification bodies provided in Article 43 of the Regulation;
- establishes the derogatory sanctioning regime, including in terms of pecuniary sanctions, applicable to public authorities and bodies, giving priority to the prevention mechanism, prior to the application of administrative fines (Article 12, Article 13 and Article 14).

57. What does it mean public authorities and bodies?

The public authorities and bodies are: Chamber of Deputies and Senate, Presidential Administration, Government, the ministries, the other specialised bodies of the central public administration, the autonomous public authorities and institutions, the local public administration authorities and at county level, other public authorities, as well as the subordinated/under coordination institutions and the cults and associations and public utility foundations, pursuant to Article 2 paragraph (1) letter a) of Law no. 190/2018.

To the extent that the concerned entity, according to the legal acts on set up, organisation and functioning, is included strictly in the definition given by the text of law, the specific provisions of Law no. 190/2018, including in terms of sanctions, become applicable.

58. Under what conditions the processing of genetic data, biometric data or data concerning health for the purpose of automated decision-making or profiling can be performed?

The processing of these categories of data for the purpose of automated decision-making or profiling **is permitted with the explicit consent** of the data subject or if the processing is carried out under explicit legal provisions, with appropriate measures protecting the rights, freedoms and legitimate interests of the data subject.

(Article 3 of the Law no. 190/2018)

59. What does it mean national identification number?

The national identification number represents the number identifying a natural person in certain record systems that is of general applicability, such as: personal numerical code, series and number of the identity card, passport number, of the driving license, social security number.

(Article 2 of the Law no. 190/2018)

60. Under what conditions can data processing be carried out on the basis of legitimate interest, including of a national identification number?

The processing of a national identification number, including the collection and disclosure of the documents that contain it, shall be performed under the conditions provided by Article 6 (1) of General Data Protection Regulation.

Where the processing of a national identification number is necessary for the purpose of achieving the legitimate interests pursued by the controller or a third party, the processing is carried out only with the establishment of the following safeguards:

- the implementation of appropriate technical and organisational measures to respect, in particular, the principle of data minimisation, as well as to ensure the security and confidentiality of personal data processing, in accordance with the provisions of Article 32 of the General Data Protection Regulation;
- the designation of a data protection officer, in accordance with the provisions of Article 10 of this law and in accordance with the provisions of Articles 37 to 39 of the Regulation;

- the setting of retention periods according to the nature of the data and the purpose of the processing, as well as specific deadlines in which personal data must be erased or revised for deletion;
- the regular training concerning the obligations of persons who, under the direct authority of the controller or processor, process personal data.

Consequently, to the extent that the legitimate interest of the controller is invoked, it should be thoroughly justified, so that it prevails over the fundamental interests, rights and freedoms of the natural persons concerned, especially as the data is to be processed. without the consent of the data subjects. The justification should be found in documentation kept by the controller.

The National Supervisory Authority may be consulted under this aspect by the controller or processor.

(Article 4 of the Law no. 190/2018)

61. Under what conditions the employees' personal data can be processed where electronic monitoring and/or video surveillance systems are used at the workplace?

Since the monitoring systems by electronic means of communication and/or by means of video surveillance entail certain risks regarding the rights and freedoms of the person, before implementing such surveillance systems, the employer should make a preliminary assessment of the risks to which its activity is submitted in order to establish the necessity of their implementation.

In accordance with the provisions of Article 5 of Law no. 190/2018, the processing of employees' personal data at the workplace by using monitoring systems by electronic means of communication and/or by means of video surveillance is allowed only if:

- a) the legitimate interests pursued by the employer are duly justified and prevail over the interests or rights and freedoms of the data subjects;*
- b) the employer has carried out the mandatory, complete and explicit information of the employees;*
- c) the employer consulted the trade union or, as the case may be, the representatives of the employees before the implementation of the monitoring systems;*

- d) other less intrusive forms and ways to achieve the goal pursued by the employer have not proven their effectiveness before; and
- e) the retention period of personal data is proportionate to the purpose of the processing, but not more than 30 days, except in cases expressly provided for by law or in cases duly justified.

The National Supervisory Authority can be consulted under this aspect.

These aspects should be found at the employer in a well-reasoned documentation, from which the prevalence of the legitimate interest over the interests or the rights and freedoms of the employees results.

For additional information you can consult *Opinion 6/2014 on the notion of legitimate interests of the controller (WP 217)* issued by the Article 29 Working Group (currently the European Data Protection Board).

(Article 5 of the Law no. 190/2018)

62. Under what conditions personal data may be processed for the performance of a task carried out in the public interest?

For the performance of a task carried out in the public interest, the processing of personal data may be carried out with the establishment by the controller or third party of the following safeguards:

- *the implementation of adequate technical and organisational measures, in particular the data minimisation, respectively the principle of integrity and confidentiality;*
- *the designation of a data protection officer (as the case may be, according to the law);*
- *the establishment of retention periods according to the nature of the data and the purpose of the processing, as well as specific deadlines in which personal data must be erased or revised for deletion.*

(Article 6 of the Law no. 190/2018)

63. Under what conditions personal data may be processed for journalistic purposes or the purposes of academic, artistic or literary expression?

The processing for journalistic purposes or for the purpose of academic, artistic or literary expression may be carried out if it concerns personal data which

have been made publicly manifested by the data subject or closely related to the person's public status or the public character of the facts in which he/she is involved, by way of derogation from the following chapters of the General Data Protection Regulation:

- a) Chapter II – Principles;
- b) Chapter III – Rights of the data subject;
- c) Chapter IV – Controller and processor;
- d) Chapter V – Transfer of personal data to third countries or international organizations;
- e) Chapter VI – Independent supervisory authorities;
- f) Chapter VII – Cooperation and consistency;
- g) Chapter IX – Specific data processing situations.

(Article 7 of the Law no. 190/2018)

64. Data subjects can exercise the rights provided for in Regulation (EU) 2016/679 in the case of processing their data for scientific or historical research purposes?

The provisions of Article 15 (**right of access** of the data subject), Article 16 (**right to rectification of data**), Article 18 (**right to restriction of processing**) and Article 21 (**right to object**) from the General Data Protection Regulation **do not apply** if personal data are processed for scientific or historical research purposes.

The **derogations** above apply to the extent that the rights mentioned in these articles are likely to make it impossible or seriously impair the achievement of the specific purposes and subject to the existence of appropriate guarantees for the rights and freedoms of the data subjects.

(Article 8 of the Law no. 190/2018)

65. Data subjects can exercise the rights provided for in Regulation (EU) 2016/679 in the case of processing their data for statistical purposes or for archiving purposes in the public interest?

The provisions of Article 15 (**right of access** of the data subject), Article 16 (**right to rectification of data**), Article 18 (**right to restriction of processing**) and Article 21 (**right to object**) from the General Data Protection Regulation **do not apply** if personal data are processed for statistical purposes or for archiving purposes in the public interest.

The **derogations** above apply to the extent that the rights mentioned in these articles are likely to make it impossible or seriously impair the achievement of the specific purposes and subject to the existence of appropriate guarantees for the rights and freedoms of the data subjects.

(Article 8 of the Law no. 190/2018)

66. Who accredits the certification bodies?

Pursuant to Article 11 of Law no. 190/2018 on implementing measures to Regulation (EU) 2016/679, the accreditation of the certification bodies, provided by Article 43 of General Data Protection Regulation, is carried out by **Romanian Accreditation Association – RENAR**, as the national accreditation body, pursuant to Regulation (EC) no. 765/2008 of the European Parliament and of Council of the 9th of July 2008, as well as pursuant to Government Ordinance. No. 23/2009 on the accreditation activity of the conformity assessment bodies, approved with amendments by Law no. 256/2011.

(Article 11 of the Law no. 190/2018)

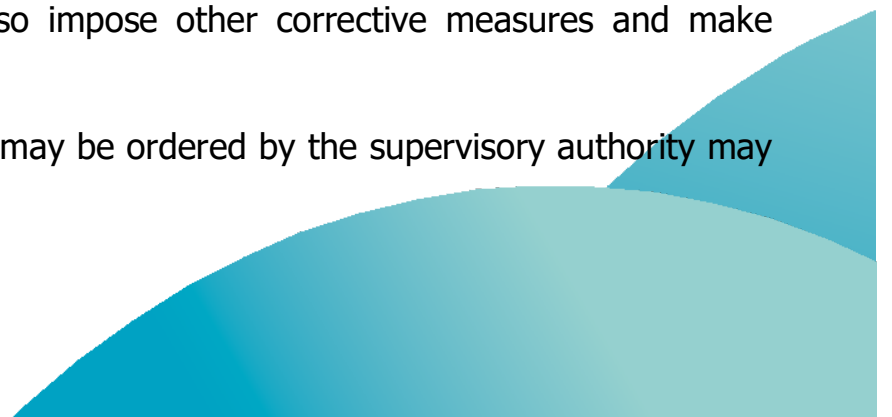
67. What measures can the supervisory authority take in the private sector if it finds a violation of the provisions of Regulation (EU) 2016/679?

The main administrative sanctions applied by the supervisory authority in the private sector are the **reprimand** and the **fine**.

Depending on the circumstances of each case, the supervisory authority imposes administrative fines of up to EUR 10,000,000 - 20,000,000 or, in the case of an enterprise, up to 2% - 4% of the total annual global turnover for the previous year, taking into account the highest value.

In addition to applying the administrative sanctions provided for by the law, the supervisory authority may also impose other corrective measures and make recommendations.

The corrective measures that may be ordered by the supervisory authority may consist of:



- obliging the controller or processor to respect the requests of the data subject for the exercise of rights, to ensure the compliance of the processing operations with the applicable legal provisions;
- obliging the controller to inform the data subject about an infringement of the protection of personal data;
- temporary or definitive limitation, ban on processing, rectification or deletion of personal data, restriction of processing;
- withdrawing a certification or ordering the certification body to withdraw a certification issued or not to issue a certification if the certification requirements are not or are no longer met;
- suspension of the data flows to a recipient in a third country or to an international organisation.

(Article 58 and Article 83 of the GDPR)

68. Public authorities and bodies may be sanctioned by the supervisory authority?

The main administrative sanctions applied to public authorities and bodies are the **reprimand and the administrative fine**.

In the event of a breach by the public authorities/bodies of the provisions of the General Data Protection Regulation and of Law no. 190/2018, the **National Supervisory Authority may impose a reprimand**, to which it shall attach a remedial plan and **it shall a deadline for fulfilling the measures ordered**.

The remedial deadline is determined based on the risks associated with the processing, as well as the steps to be taken in order to ensure compliance of the processing.

The remedial plan is provided in the Annex to Law no. 10/2018. This is an annex to the report of finding and sanctioning of the contravention.

Where the supervisory authority finds that the public authorities/bodies have not fully complied with the measures provided in the remedial plan, within the deadline set by the authority, it may apply **the administrative sanction of the fine from 10,000 lei up to 200,000 lei**.

(Article 13 and Article 14 of the Law no. 190/2018)

69. What administrative decisions with normative character the

National Supervisory Authority issued in 2018?

In order to implement the Regulation (EU) 2016/679, the National Supervisory Authority has issued the following administrative decisions with normative character:

- **Decision no. 99/2018** regarding the cessation of the applicability of normative acts of administrative character issued in application of Law no. 677/2001 for the protection of persons regarding the processing of personal data and the free movement of these data
- **Decision no. 128/2018** regarding the adoption of the standardised form for the notification of personal data breach, in accordance with 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
- **Decision no. 133/2018** on the approval of the Procedure for receiving and solving complaints
- **Decision no. 161/2018** on the approval of the Procedure for performing investigations
- **Decision no. 174/2018** on the list of kind of processing operations which are subject to the requirement for a data protection impact assessment.

Also, Decision no. 184/2014 regarding the approval of the standardised form for the notification of the personal data breach by the providers of public services of electronic communications networks or services, in accordance with Regulation (EU) no. 611/2013 of the Commission of 24 June 2013 on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and the Council on privacy and electronic communications (published in Official Journal no. 964 of 30th of December 2014).

70. What are the main issues covered by Decision no. 133/2018 regarding the approval of the Procedure for receiving and solving complaints?

Decision no. 133/2018 on the approval of the Procedure for receiving and solving complaints mainly concerns the following issues:

- ✓ **complaints may be addressed by any data subject**, especially if his/her habitual residence, place of work or alleged violation is or, as the case may be, takes place on the territory of Romania;

- ✓ complaints may be submitted to the Supervisory Authority's premises or sent by post, including electronic mail, or by using the electronic complaint form available on the institution's website https://www.dataprotection.ro/index.jsp?page=Plangeri_RGPD;
- ✓ **complaints may be filed personally or by the representative** of the data subject, including through a organisation without patrimonial purpose, active in the field of the protection of personal data;
- ✓ **the petitioners are informed in writing of the admissibility of the complaint**, including the carrying out of a more thorough investigation or coordination with other supervisory authorities, as well as of the evolution or outcome of the investigation undertaken;
- ✓ **the data subject dissatisfied with the way of solving his/her complaint can address the administrative contentious section of the competent court**, after having completed the preliminary procedure provided by the Law of the administrative contentious no. 554/2004, as subsequently amended and supplemented

71. Who can submit a complaint to the supervisory authority?

Any data subject who considers that the processing of his/her personal data violates the legal provisions in force, especially if his/her habitual residence, place of work or alleged violation is or, as the case may be, takes place on the territory of Romania can submit a complaint.

72. What are the conditions for filing in a complaint??

Complaints should be addressed in writing, in Romanian or English.

The complaints may be filed at the general registry at the premises of the supervisory authority or may be sent by post, including electronic mail, or by using the electronic form available on the supervisory authority's website, under section Complaints.

Prior to submitting a complaint to the supervisory authority, the data subjects may exercise the rights provided for in Chapter III of the Regulation (EU) 2016/679. According to Article 12 paragraph (3) of the GDPR, the controller shall provide the data subject with information on the actions taken following a request under Articles 15 to 22, without undue delay and in any case *no later than one month after receiving the request*.

For additional information, we recommend you to consult *Decision no. 133/2018 of the president of the National Supervisory Authority on the approval of the Procedure for receiving and solving complaints*, available on the website of the authority www.dataprotection.ro.

73. The complaints can be filled in also by other persons that the data subject?

The complaints shall be submitted personally or by a representative, with the attachment of the power of attorney issued according to the law or of a notary proxy, as the case may be.

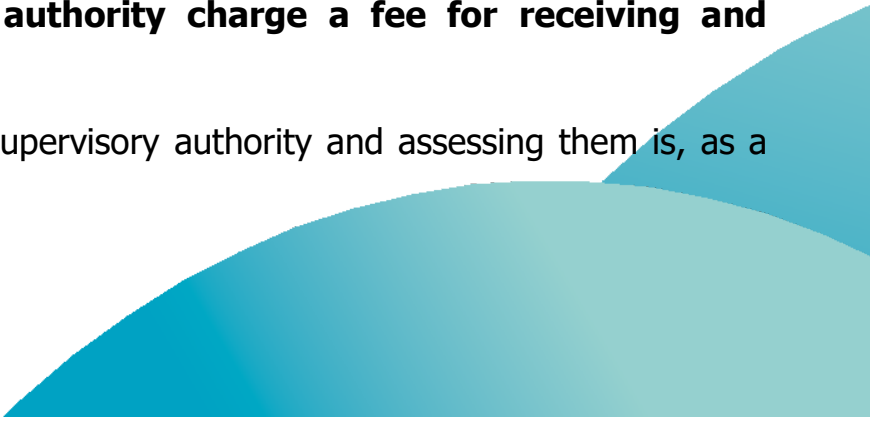
The complaints may also be filed by the representative of the data subject who is a spouse or relative up to second degree inclusive, by attaching a declaration on own responsibility signed by the petitioner, and for the case of other persons, the notary proxy.

The complaints can be filed also through a body, organization, association or foundation without patrimonial purpose. They must prove that they have been legally constituted, with a statute providing for public interest objectives, and that they are active in the field of the protection of the rights and freedoms of data subjects with regard to the protection of their personal data. In this case, the complaint shall also include the power of attorney or the notary proxy of representation, as the case may be, in order to show the limits of the mandate given by the data subject and the statute of the body/organization/association/foundation, as well as the evidence of their activity in the field of the protection of the data subjects' rights and freedoms with regard to the protection of their personal data.

For additional information, we recommend you to consult *Decision no. 133/2018 of the president of the National Supervisory Authority on the approval of the Procedure for receiving and solving complaints*, available on the website of the authority www.dataprotection.ro.

74. May the supervisory authority charge a fee for receiving and assessing the complaints?

Receiving complaints by the supervisory authority and assessing them is, as a rule, free of charge.



Where the complaints are manifestly unfounded or excessive, in particular because of their repetitive nature, *the supervisory authority may charge a reasonable fee* based on administrative costs or may refuse to treat them.

For additional information, we recommend you to consult *Decision no. 133/2018 of the president of the National Supervisory Authority on the approval of the Procedure for receiving and solving complaints*, available on the website of the authority www.dataprotection.ro.

75. May the petitioners request the confidentiality of certain personal data?

The petitioners may request the confidentiality of certain expressly mentioned personal data provided through the complaint, except for the cases where, for the proper solving of the subject matter of the complaints submitted, the petitioner's identification data must be disclosed to the complainant entity.

For additional information, we recommend you to consult *Decision no. 133/2018 of the president of the National Supervisory Authority on the approval of the Procedure for receiving and solving complaints*, available on the website of the authority www.dataprotection.ro.

76. When a complaint is admissible?

For the receipt and valid registration of the complaints, *it is mandatory* to provide the following data of the *petitioner*: name, surname, postal address of domicile or residence.

If the complaint is filed electronically, it is mandatory to provide the petitioner's e-mail address.

In the case of complaints submitted by a representative, beside the data of the petitioner it is also mandatory to provide the following data of the representative: *name and surname/name, postal address of correspondence/headquarters, e-mail address, telephone number, registration number in the register of associations and foundations*, if applicable.

For valid receipt and registration of complaints, *it is mandatory* to provide the identification data of the *complainant controller* or processor, such as name and surname/name, address/headquarters, or at least the available information held by the petitioner for identification.

The submitted complaints *shall be signed by handwriting or by electronic means*, and, in the case of electronically submitted petitions that cannot be signed, the National Supervisory Authority may request the confirmation of the correctness of the data transmitted electronically.

For additional information, we recommend you to consult *Decision no. 133/2018 of the president of the National Supervisory Authority on the approval of the Procedure for receiving and solving complaints*, available on the website of the authority www.dataprotection.ro.

77. What is the deadline for the supervisory authority to provide an answer to complaints?

The national supervisory authority shall inform the data subject about the admissibility of the complaint, within 45 days from the registration.

If it is found that the information in the complaint or the documents transmitted are incomplete or insufficient, the National Supervisory Authority requests the data subject to complete the complaint in order to be considered admissible for the purpose of carrying out an investigation. A new deadline of no more than 45 days starts from the date of filing the complaint.

The national supervisory authority shall inform the data subject about the progress or outcome of the investigation, within three months from the date on which it was notified that the complaint is admissible.

For additional information, we recommend you to consult *Decision no. 133/2018 of the president of the National Supervisory Authority on the approval of the Procedure for receiving and solving complaints*, available on the website of the authority www.dataprotection.ro.

78. Do the data subjects have the right to address the competent court to defend the rights that have been violated?

Without prejudice to the possibility of addressing a complaint to the National Supervisory Authority, the data subjects have the right to address the competent court to defend the rights guaranteed by the applicable law which have been violated.

If a claim has been filed with the same object and having the same parties, the

supervisory authority *may order the suspension and/or classification of the complaint*, as the case may be.

The data subject will have to inform the Authority, through the complaint form, about the filing of such an application in court.

79. Under what conditions does the Regulation (EU) 2016/679 apply to complaints and intimations filed and registered with the supervisory authority?

The provisions of the General Data Protection Regulation apply to:

- ✓ *complaints and intimations filed and registered at the National Supervisory Authority after the 25th of May 2018;*
- ✓ *complaints and intimations filed before the 25th of May 2018 and currently being handled;*
- ✓ *investigations carried out to solve complaints and intimations and ex officio investigations, including those started before the 25th of May 2018 and not finalised at this date.*

(Article VI of the Law no. 129/2018)

80. When can a complaint be classified?

The complaint that does not specify the identification data of the petitioner (name, surname, postal address of domicile or residence) is considered anonymous and is classified with this mention, without a reply to the petitioner.

For additional information, we recommend you to consult *Decision no. 133/2018 of the president of the National Supervisory Authority on the approval of the Procedure for receiving and solving complaints*, available on the website of the authority www.dataprotection.ro.

81. What aspects does the Decision no. 161/2018 on the approval of the Procedure for performing investigations regulates?

Decision no. 161/2018 on the approval of the Procedure for performing investigations establishes the conditions for conducting investigations on spot, at the premises of the supervisory authority and those carried out in writing, as well as their performance at public authorities/bodies.

The investigation can be finalised by drawing up a report of the

finding/sanctioning or a decision of the president of the National Supervisory Authority, through which corrective measures and/or administrative sanctions (reprimand, fine) can be imposed.

In the case of public authorities/bodies, prior to imposing a pecuniary sanction, a reprimand is applied and a remedial plan is drawn up according to the model provided by Law no. 190/2018 and which should be fulfilled within the period granted by the supervisory authority. The measures ordered can be appealed within 15 days at the administrative litigation section of the competent court.

For additional information, we recommend you to consult *Decision no. 161/2018 of the president of the National Supervisory Authority on the approval of the Procedure for performing investigations*, available on the website of the authority www.dataprotection.ro.

82. When does the supervisory authority conduct investigations?

The supervisory authority carries out investigations ex officio or following a complaint.

The ex officio investigations are carried out for the verification of certain data and information regarding the processing of personal data, obtained by the National Supervisory Authority from sources other than those that are subject to complaints.

The investigations can also be carried out to solve the complaints received by the National Supervisory Authority.

For additional information, we recommend you to consult *Decision no. 161/2018 of the president of the National Supervisory Authority on the approval of the Procedure for performing investigations*, available on the website of the authority www.dataprotection.ro.

83. How is the investigation carried out?

The investigations can be carried out on spot, at the authority's premises or in writing.

On spot investigations consist of verifications carried out at the premises/domicile/working point or other locations where the controlled entity carries out its activity or locations related to the processing in question, as the

case may be.

The investigation cannot begin before 08:00 and cannot continue after 18:00 and should be carried out in the presence of the person where the investigation is carried out or of its representative. The investigation can continue after 18:00 only with the consent of the person where the investigation is performed or of its representative.

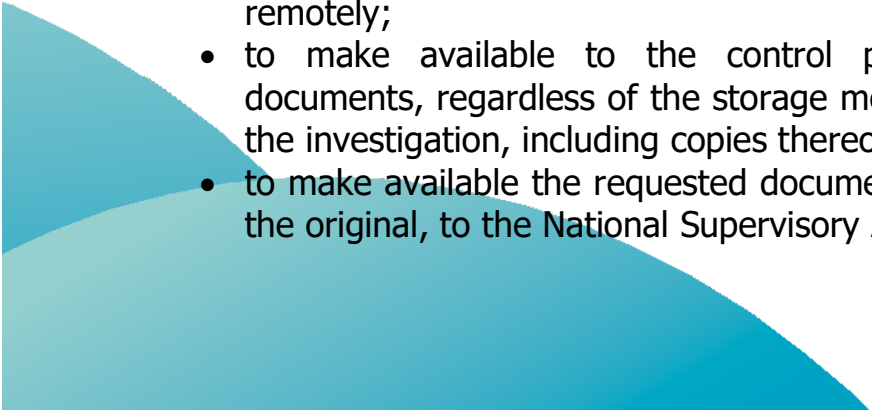
In the case of investigations carried out at the premises of the National Supervisory Authority, the designated control personnel sends an letter of summons of the representatives of the controlled entity, specifying the date and time of commencement of the investigation.

In the case of written investigations, a letter is sent to the controlled entity, requesting information, data and documents necessary to solve the case under investigation.

For additional information, we recommend you to consult Decision no. 161/2018 of the president of the National Supervisory Authority on the approval of the Procedure for performing investigations, as well as Chapter IV of Law no. 102/2005, republished, available on the website of the authority www.dataprotection.ro.

84. What are the obligations of the controlled entity in case of on spot investigations?

During the on spot investigation, the controlled entity has, in principal, the following obligations:

- to allow the control personnel, without delay, to start and conduct the investigation and to provide the necessary support to the control personnel;
 - to ensure the access of the control personnel in the premises where they carry out their activity, to any equipment, means or support for data processing/storage, in order to carry out the necessary checks for performing the investigation, including those that can be accessed remotely;
 - to make available to the control personnel any information and documents, regardless of the storage medium, necessary for carrying out the investigation, including copies thereof;
 - to make available the requested documents, certified for compliance with the original, to the National Supervisory Authority;
- 

- to provide in a complete form the requested documents, information, records and evidences, as well as any necessary explanations, without being able to oppose their confidential character, according to the law;
- to allow the control personnel to use the audio-video/photo recording and storage equipment whenever the control team considers it necessary in the conduct of the control activity.

The controller or processor may file an appeal with the administrative contentious section of the competent court against the minutes of finding/sanctioning and/or the decision to impose the corrective measures, as the case may be, within 15 days from the handing, respectively from the communication. The decision solving the appeal can be challenged only by appeal. The appeal is judged by the competent court of appeal. In all cases, the competent courts are those in Romania.

For additional information, we recommend you to consult Decision no. 161/2018 of the president of the National Supervisory Authority on the approval of the Procedure for performing investigations, as well as Chapter IV of Law no. 102/2005, republished, available on the website of the authority www.dataprotection.ro.

85. How are considered the references to Law no. 677/2001 from the national legislation?

All references to Law no. 677/2001, with the subsequent amendments and completions, from the national normative acts are interpreted as references to the General Data Protection Regulation and to the law for its implementation.





AUTORITATEA NAȚIONALĂ DE SUPRAVEGHERE A PRELUCRĂRII DATELOR CU CARACTER PERSONAL



romania2019.eu
Președinția României la Consiliul Uniunii Europene

