March – June 2017

Balcar, Polanský & Spol. s.r.o.'s

School of Data Protection

Regulation (EU) 2016/679 of the EP and of the Council of 27 April 2016, the General Data Protection Regulation (the "GDPR") replaces Directive 95/46/EC (the "Directive"), which currently forms part of Slovak law through Act no. 122/2013 Coll. and part of Czech law through Act no. 101/2000 Coll., the Data Protection Act. The GDPR will come into effect on 25 May 2018, when it will be directly applicable throughout the EU. It will apply to those who process personal data, as well as to natural persons whose personal data is the subject of processing.

To help you navigate the maze of obligations introduced by the GDPR, we have created a regular weekly news series on this topic, which is without a doubt the most important legislative change in European history in the field of data protection.

Lesson 1 of 16

Material and territorial scope of the GDPR

Below you will learn:

Important changes

- The GDPR will have a significantly broader impact on those who process personal data.
- The GDPR will also apply to businesses/institutions which are not established in the EU;
    - if they process the personal data of data subjects located in the Union in relation to offering goods or services to them, irrespective of whether a payment is required, or
    - in relation to the monitoring of their behaviour if it takes place within the Union (e.g. through technical equipment such as *cookies*).

Compliance Action Plan

- Businesses/institutions should assess whether the GDPR will apply to them.
- If yes, we will provide information on a weekly basis about how to ensure compliance and minimize the risk of high sanctions.
- If not, we recommend implementing continuous monitoring processes to ensure this status into the future.

Material scope

The GDPR applies to the processing of personal data:

- carried out wholly or partly by automated means (mostly through IT means) and to;
- processing other than by automated means (e.g. entries in paper form) of personal data which:
    - form part of a filing system, or
    - are intended to form part of a filing system.

The GDPR does not apply to some types of processing, e.g. for personal or household purposes, internal security of Member States, etc.

Most of processing operations in the public and especially in the commercial sphere will be subject to the GDPR.

Territorial scope

Controllers and processors "established" in the EU

First of all, the GDPR will apply to persons and businesses that are "established" in the EU, if they process personal data in the context of their activities. It is a broadly defined rule which aims to ensure that the GDPR applies to controllers[1] and processors[2] processing personal data, if they are established in the EU, regardless of whether the processing takes place in the Union or not.

It is important to note that the GDPR extended its scope in connection to processors established in the Union. Pursuant to the previous legislation, if the controller was not established in the EU but

[1] who alone or jointly with others determines the purposes and means of the processing of personal data.
[2] who processes personal data on behalf of the controller.

appoints a processor established in the EU to process personal data on their behalf, such processing does not fall within the scope of the Directive.

A new crucial circumstance is that the concept of "establishment" of a business in the EU was defined more clearly by recent decisions of the EU Court of Justice ("CJEU"). Quite revolutionary in this regard is especially the CJEU's decision in *Weltimmo v. NAIH* from 2015 (C-230/14), which has an enormous impact on persons doing business through the internet in several EU States. The company Weltimmo had its registered office in Slovakia and provided services through the internet on a cross-border basis to Hungarian citizens. The CJEU decided that the Slovak company, despite not having a branch or other form of entrepreneurship in Hungary, is subject to the decisions of the Hungarian authority supervising the protection of personal data. The CJEU articulated that if a company offers services in the official language of a particular State (in this case in Hungary) and has a representative in the said country, in such case it underlies the supervision power of authorities in this country regardless of the fact that it is not registered in the local commercial or other register. In the CJEU's opinion, the existence of a subsidiary of a company in a particular state is not a necessary criterion for assessing whether a company is established in such country or not. On the contrary, establishment may arise where the company carries out real and effective activity, however minimal, through e.g. a web page in the local language, a representative operating in the respective territory and possibly a post box or a bank account, such as in the case of Weltimmo.

Businesses not established in the EU

The extension of the territorial scope of the GDPR to companies not established in EU Member States, but processing the personal data of persons located in the Union, is one of the most important changes introduced by the GDPR. If a company or an institution with its registered office outside of the Union meets one of the conditions set out by the GDPR, the Regulation will automatically apply to its processing activities. Such person will be obliged to comply with the principles of processing and to implement measures for ensuring the safety of personal data as outlined by the GDPR. They will be subject to the supervision powers of bodies determined by the GDPR and bear any potential sanctions such bodies impose.

The GDPR will apply to controllers and processors not established in the Union if they process the personal data of data subjects located in the Union, and if the processing activities are related to:

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

What exactly is meant by "data subjects who are in the Union" is not quite clear yet. However, we can assume that it will be a broad concept and there will be a tendency to interpret it in a way to include as many data subjects as possible under the "umbrella" of the protection provided by the GDPR. Decisive criteria for the interpretation of this term might be the data subject's place of physical presence or place of residence.

For the first time, the scope of the Regulation is based on whether a company monitors the behaviour of persons on the territory of the Union. Monitoring will probably be most frequently carried out through the internet by means of small text files sent by the collector of the data to the data subject's equipment (smartphone, computer etc.), so called cookies.

Under the previous legal regulation pursuant to the Directive the supervisory bodies strived to establish their supervision power over non-EU businesses processing the personal data of EU citizens through the fact that businesses used technical equipment located in the EU for the processing of personal data, whereby this technical equipment was cookies. Pursuant to the GDPR, these efforts will not be necessary anymore due to an unambiguous provision on the applicability of

the GDPR if the company monitors the behaviour of data subjects who are in the Union. Further processing will become relevant as well, especially profiling, which is defined as any form of automated processing of personal data consisting of the use of personal data to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

When assessing if a non-EU company is considered as established in the Union, the criteria mentioned above articulated by the CJEU in its decision *Weltimmo v. NAIH* will be decisive. That means that the mere fact that a certain web page can be viewed from an EU country will not be sufficient for the conclusion about the existence of the establishment in the EU. For this conclusion the activities of the business should be provably aimed at data subjects located in the EU. If web pages are designed also in (at least) one of the local EU languages, contain pricing in one or more local currencies (e.g. GBP, EUR, CZK), contain contact details such as telephone numbers with European country codes, such circumstances would be relevant for the conclusion that the establishment of the business in the Union exists.

The extent to which European authorities will supervise the processing of personal data by companies outside of the EU has not been tested so far. The actual enforceability of their decisions aimed at companies outside the EU (e.g. the decision of the Slovak Data Protection Authority to imposing a fine on a Chinese company) is still questionable. However, the concept of protection of data subjects in the Union in relation to companies outside the EU is revolutionary. The rationale behind its introduction was the conviction that data subjects in the EU should not be deprived of due protection in relation to the processing of their personal data just because a company is headquartered elsewhere.

What now

First of all, businesses and institutions should find out whether the GDPR will apply to them with regard to the extended territorial scope. Non-EU businesses should exercise caution when assessing whether they are considered as "established" in the EU.

If the activities of a business or an institution fall under the scope of the new Regulation, it will be crucial to get to know the numerous obligations set out by the GDPR and to train staff that will on behalf of the business or the institution handle personal data. The obligations of controllers and processors, data subject's rights and basic principles for processing personal data will be the subject of the next lessons of the School of Data Privacy.

Further information can be found here

Material scope:	Recitals 6-18 of the GDPR; article 2 of the GDPR
Territorial scope:	Recitals 22-24 of the GDPR; article 3 of the GDPR

Lesson 2 of 16

Data Protection Principles

Below you will learn:

Important changes

- As a result of the new accountability principle, companies / institutions processing personal data on their own behalf (controllers) will not only have to comply but also be able to demonstrate that they process personal data in compliance with data protection principles.

Compliance Action Plan

Prior to the GDPR taking effect, controllers should:

- audit the processing of personal data aimed at new obligations;
- create (or update existing) internal rules regulating processing, update the work rules regarding employee monitoring and protection of their personal data, revise employment contracts of employees having access to personal data as well as other documents related to processing;
- ensure and be able to demonstrate employees authorised to access personal data are trained regarding their rights, obligations and the consequences of breaches in relation to themselves and the employer.

Regarding Data Protection Principles

The data protection principles set out by the GDPR are similar to those outlined by the Directive, which are contained in Act no. 122/2013 Coll. and in Act no. 101/2000 Coll., the Data Protection Act. However, the GDPR further specifies and extends them.

Lawfulness, Fairness, Transparency

Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.

For purposes of the transparency principle, companies / institutions will have to comply with the obligation to provide data subjects, whose personal data they process, with an extensive package of information. They should inform the data subjects in a clear and understandable manner on the conditions of processing and the rights the data subjects enjoy in relation to this[3].

In comparison to the Directive, the list of information that the controllers must demonstrably provide to data subjects prior to processing is significantly broader and among other things includes the right to erasure (i.e. right to be forgotten[4]), the right to object and to file a complaint

[3] Secret and invisible installed spyware is considered to be illegitimate processing (see the case of a website operator who publishes the e-mail addresses of participants in an internet discussion; WP 29 the Working party on the protection of individuals with regard to the processing of personal data).

[4] So far this has only been judicially laid down by the CJEU, see C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González. The dispute between Google and P. González, who wished to erase an unpleasant episode from the public consciousness; in the press was published information about the forced sale of his property because of an outstanding debt to social insurance, which was subsequently repaid. The Spanish office has ordered Google Inc. to take the necessary measures to remove the personal data relating to p. González from its index and prevent access to that information in the future.

with the supervisory authority and the right not to be subject to a decision based solely on automated processing, including profiling[5]. Needless to say, among the information on one's rights, data subjects must be notified of the conditions of processing, including the purposes of processing and the legal grounds (e.g. consent, legal requirements, etc.). We will cover the notification obligation in a separate Lesson.

Purpose limitation

Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes[6]. In contrast to the actual legislation, further processing for another purpose than that for which the personal data was collected will be permissible under certain conditions. This is a substantial change in Czech and Slovak conditions of processing and means that if the controller collected personal data for a specific purpose, they may process such data for other purposes, if they meet certain conditions.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes are not considered to be incompatible with the initial purposes. However, this applies only if the controller ensures appropriate safeguards for data subject's rights and freedoms. For this purpose, the controller or processor should adopt technical and organisational measures such as data minimisation, pseudonymisation[7] or anonymisation.

From our point of view, the processing of personal data collected while dealing with an offense for secondary purposes such as e.g. publishing in a local periodical or via the Internet, or publishing information about the existence of a debt of the owner of an apartment which was primarily processed with respect to administrative issues regarding the house, or disclosure of the collected personal information of individual tour participants to other passengers without their consent, will continue to be considered processing incompatible with the primary purpose.

Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

The adequacy of personal data in relation to the purpose of processing is not always easily defined. To determine whether the processing of certain personal data is adequate will require assessing whether the invasion of data subject's rights, which will occur as a result of processing, is adequate to the legitimate purpose of processing. If the processing of certain personal data for a specific purpose proves excessive, such processing would not be compliant with the GDPR. For example, it would be obviously inadequate to process a data subject's birth number for marketing purposes, since this it is not necessary to process this information for such purpose.

---

[5] See Article 4, para. 4 of the GDPR, i.e. "*any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*".

[6] I.e. it is a general prohibition of further processing for secondary purposes, incompatible with the primary purpose, whereas "*compatibility*" means "*direct relation*" to the primary purpose.

[7] See Article 4, para. 5 of the GDPR, i.e. *"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."*

Accuracy

Personal data must be accurate and, where necessary, kept up to date. The controller must ensure that inaccurate personal data is erased or rectified without delay.

Storage limitation

Personal data must be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 subject to implementation of the appropriate technical and organisational measures required by this Regulation, in order to safeguard the rights and freedoms of the data subject.

The opinion of the Czech Data Protection Authority, under which operating a camera system at a permanently protected private facility the permissible time limit is e.g. 24 hours (but not exceeding several days), will still be valid. Restrictions will not apply to records acquired by the Czech Police under special legislation or in the event of a security incident when the record will be provided as evidence to the competent authorities for further proceedings.

Integrity and confidentiality

Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Accountability

The controller is responsible for processing personal data in line with the principles explained above, and he/she must be able to demonstrate compliance. To demonstrate compliance, it is possible to execute written documents stating that all aspects of the processing operations within the company or the institution were internally assessed, and the result of the assessment was compliance with the GDPR's provisions.

The GDPR introduces new concepts of *data protection by design* and *data protection by default.*

Data protection by design means that the controller, with regard to various aspects of processing (e.g. the state of the art, the nature, scope, and purposes of processing, risks arising to the data subject's rights) must prior to the start of processing adopt appropriate technical and organisational measures and safeguards for the protection of personal data, and to adapt these from time to time to the actual conditions of processing. In other words, this concept obliges all companies / institutions processing personal data to carry out an internal audit of processing personal data. This requires controllers to proactively deal with the protection of personal data and to set aside human resources and financial and technical resources to assess the lawfulness of the processing and implement measures for its protection.

Data Protection by default means that the controller ensures only the personal data that is necessary for each specific processing purpose is processed. They should ensure that by default, personal data is not made accessible, without the individual's intervention, to an indefinite number of natural persons.

If the controller processes personal data through another person (processor), such person is obligated to process personal data only based on the controller's instructions, unless required to do so by Union or Member State law.

What now

All concerned companies / institutions should carry out an audit of processing personal data to ensure compliance, but also to ensure that they have the ability to demonstrate that personal data is processed with professional care, and to adopt organisational and technical measures and safeguards for this purpose. Suggestions for ensuring this can be found above in the part Compliance Action Plan.

Further information can be found here

Recitals 39, 40, 22

Articles 5, 6, 24, 25, 29, 89(1)

Lesson 3 of 16

Lawfulness of processing and further processing

Below you will learn:

Important changes

- The GDPR changes the legal grounds for processing personal data
- In certain cases, processing for a different purpose than the purpose for which the personal data was originally collected will be permitted
- New criteria have been introduced for the compatibility test for the purposes of processing

Compliance Action Plan

- Checking the legal grounds for processing personal data and ensuring that they will be relevant after the GDPR comes into effect
- Ensuring the ability to demonstrate a compatibility test if personal data is processed for reasons other than the original purpose

Regarding the lawfulness of processing

As we mentioned in Lesson 2, one of the principles relating to processing personal data is the lawfulness of processing[8]. The term "lawfulness" is fairly broad and without further clarification it would be vague and legally uncertain. The GDPR further regulates it in clause 6.

The principle of lawfulness means that if no exception regulated by the GDPR applies to the processing, the controller is always obligated to obtain the data subject's consent with the processing of his/her personal data. Besides the data subject's consent, which is the basic legal ground for the processing and will be discussed in a separate lesson, processing will be lawful only if and to the extent that at least one of the following applies ("legal grounds for processing")[9]: if the processing is necessary:

a) 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[10];

b) for compliance with a legal obligation to which the controller is subject[11];

c) in order to protect the vital interests of the data subject or of another natural person[12];

---

[8] Art. 5(1) of the GDPR: *Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject*

[9] The lawfulness of processing sensitive data will be the subject of a separate lesson.

[10] E.g. a consumer orders goods through an on-line shop, the seller needs to process his/her name, surname, address or another contact details for the purpose of delivery.

[11] The basis for the processing must be laid down by Union law or Member State law to which the controller is subject. Such law can regulate concrete circumstances of processing such as the general conditions governing the lawfulness of processing by the controller, the types of data which are subject to the processing, the data subjects concerned, the entities to, and the purposes for which, the personal data may be disclosed, the purpose limitation, storage periods, and processing operations and procedures, including measures to ensure lawful and fair processing.

[12] Processing of personal data based on the vital interest of another natural person should take place only where the processing cannot be manifestly based on another legal basis.

d) for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller[13];

e) 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 requiring personal data protection, in particular where the data subject is a child[14].

Besides the data subject's consent, the most relevant issue for businesses will be the legal grounds for processing outlined in point a), b) and e) above.

The GDPR allows States to add additional specific requirements and implement measures for processing care of the reasons outlined in points b) and d) above. The same is allowed in other special situations where the processing takes place[15].

The legal grounds for processing as of the effective date of the GDPR will include:

- in relation to Article 85 of the GDPR, processing of personal data necessary for academic, artistic, literary or journalistic purposes, if it arises from the controller's business activities, except if such processing would violate the data subject's right to protection of his/her personality and privacy or if such processing without the data subject's consent is prohibited by a special Act or an international treaty;
- in relation to Article 88 of the GDPR, providing access to, providing or publishing of personal data in the extent of academic title, name, surname, work/service position or function, department, place of work, telephone number, fax number or work e-mail address and the employer's identification details provided that the controller is the data subject's employer;
- in relation to Article 87 of the GDPR, processing of a national identification number regulated by a special Act for the purpose of determining a natural person only if its use is necessary for reaching the respective purpose of processing and if the data subject gave his/her written or otherwise demonstrable consent for processing thereof;
- in relation to Article 89 of the GDPR, processing for the purposes of archiving in the public interest, scientific or historical research or for statistical purposes;
- in relation to Article 49(5) of the GDPR, the entitlement of transferring a special category of personal data and the national identification number to a third party located in a third country which does not ensure an adequate level of personal data protection only with the prior explicit consent of the data subject, unless a special Act provides otherwise;
- in relation to Article 9(4) of the GDPR, processing of genetic data, biometric data and data related to health, if it is necessary for compliance with a legal obligation to which the controller is subject.

It will always remain the obligation of the States to ensure personal data protection complies with the right to freedom of expression and information in these special cases.

States are also obliged to notify the Commission before the GDPR enters into force about detailed rules, nuances and exceptions to the processing of personal data for journalistic purposes and for purposes of academic, artistic or literary expression, for processing in the context of employment and in the context of the statutory duty of confidentiality.

[13] As in footnote no. 4.

[14] The existence of a legitimate interest needs careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could, in particular, override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

[15] As stated in Chapter IX of the GDPR.

Obsolete legal grounds

In comparison to the valid legislation[16] ("the Act") when the GDPR takes effect the following legal grounds will be abolished:

- legal ground pursuant to Art. 10(3) let. d) of the Act "direct marketing in postal traffic"; while adhering to the conditions regulated by the GDPR, especially the proportionality principle with regard to reasonable expectations of data subjects and with regard to the existence of the controller's legitimate interest, direct marketing will be able to be regarded as a legitimate interest (ie the legal ground sub e) above);
- legal ground pursuant to Art. 10(3) let. e) of the Act "further processing of published personal data"; this legal ground is in conflict with the lawfulness, fairness and transparency principle, the principle of purpose limitation and purpose compatibility; when processing published personal data, the controller will have to comply with a relevant legal ground; and
- legal ground pursuant to Art. 15(4) of the Act "one-time entry" and legal ground pursuant to Art. 15(7) of the Act "monitoring of publicly accessible premises"; the controller will have to comply with a relevant legal ground, e.g. a legal obligation pursuant to point b) above or a legitimate interest pursuant to point e) above.

Regarding the lawfulness of further processing

As we mentioned in Lesson 2, another principle relating to personal data processing is the limitation of purpose. It binds controllers to collect personal data for specified, explicit and legitimate purposes and prohibits them to further process it in a manner that is incompatible with those purposes.[17] However, in Article 6 sec. 4 the GDPR permits that personal data, collected for a specific purpose, may be under specific conditions processed for a purpose different than the original one ("further processing"). It is processing for a different purpose but compatible with the original one, on the basis of the same legal ground (ie the purpose is different, the legal ground remains).

By this provision the GDPR literally brings light to a grey zone which existed in the issue of further processing under the previous legal regulation. The GDPR explicitly regulates that further processing for privileged purposes (ie archiving in the public interest, scientific or historical research or statistical purposes) is not incompatible with the original purpose if the controller ensures appropriate safeguards for the rights and freedoms of the data subject.[18] Besides that the GDPR also lays down the factors controllers must take into account when accessing whether the new purpose is compatible with the purpose for which it was originally collected.

In other words, if the controller considers whether they may process personal data for a different purpose than for which it was originally collected, they are obliged to carry out a compatibility test with the purposes of processing. The compatibility test is carried out with regard to specific conditions such as:

- any link between the purposes for which the personal data was collected and the purposes of the intended further processing;
- the context in which the personal data was collected (in particular regarding the relationship between data subjects and the controller);

[16] Act no. 122/2013 Coll., the Data Protection Act as amended (Slovakia).

[17] Art. 5(1) let. b) of the GDPR: *Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*

[18] For this purpose the controller should implement technical and organisational measures which can include data minimisation, pseudonzmisation or anonymisation.

- the nature of the personal data (in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed);
- the possible consequences of the intended further processing for data subjects;
- the existence of appropriate safeguards (e.g. encryption or pseudonymisation).

The GDPR introduces the above criteria with the phrase "inter alia", which means that other suitable criteria may be taken into account for the purpose of the compatibility test. However, if the processing for the original purpose is based on the data subject's consent or based on special legislation (regulating e.g. public interest, national or public security, etc.) the controller should be allowed to further process the personal data irrespective of the compatibility of purposes.

The conditions for admissibility of further processing relate only to the original controller. Should the processing operation result in providing personal data to another controller, they would also have comply with a separate legal ground for processing. Also, the controller is obligated to inform data subjects in advance of any instances of further processing.

What now

In relation to the new legal regulation outlined above it is vital that prior to the GDPR taking effect businesses and institutions check that they process personal data based on the legal grounds regulated by the GDPR.

It will also be necessary to conduct a compatibility check under the relevant criteria to ensure the lawfulness of further processing.

Further information can be found here

Recitals 40, 41, 44 - 47, 50, 153, 155

Articles 5 sec. 1 let. a) and b), 6, 23 sec. 1, Chapter IX (Articles 85-91)

Lesson 4 of 16

Consent with processing personal data

Processing the personal data of children

Below you will learn:

Important changes

- The GDPR brings new requirements for giving consent with processing personal data
- There are specific requirements regarding processing the personal data of persons in relation to scientific research and children's[19] data

Compliance Action Plan

- Businesses and institutions should ensure that they process personal data based on relevant and existing legal grounds
- If personal data is processed based on consent, it is necessary to ensure that:
    - consent is given by the data subject actively, not by silence, inactivity or pre-ticked boxes;
    - consent is distinguishable from other agreements, it is specific and clear;
    - data subjects are informed of the possibility to withdraw the consent at any time and it must be as easy to withdraw consent as to give it;
    - the provision of services must not be conditional on consent to the processing of personal data that is not necessary to perform the contract;
    - separate consents are given for distinct processing operations;
    - consent is not given in a situation of clear imbalance between the controller and the data subject (e.g. where the controller is a public authority).

Regulation of consent in the processing personal data

As we mentioned in Lesson 3, if no exception regulated by the GDPR applies to the processing of personal data, the controller must always obtain the data subject's consent with processing his/her personal data. The GDPR defines the consent as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her[20].

Pursuant to current Slovak legislation[21], consent is defined as any freely given, *express* and intelligible manifestation of will, so the new legislation differs from the current one *inter alia* in that the GDPR does not require express consent. That means that the consent can be implied (e.g. given by a certain action, but not omission), but it must be given freely, it must be specific, clear and based on intelligible information given to the data subject. In comparison, the current Czech legislation[22] defines consent only as any freely given and deliberate manifestation of will, the

[19] The GDPR uses the term "child"; a Czech and Slovak equivalent can also be a "minor".
[20] Article 4 (11) of the GDPR.
[21] Article 4 (3) let. d) of the Slovak Act no. 122/2013 Coll., the Data Protection Act, as amended.
[22] Article 4 let. n) of the Czech Act no. 101/2000 Coll., the Data Protection Act, as amended.

content of which is the data subject's consent to the processing of personal data. The new legislation thus states expressly that the consent can be implied (under conditions described above). The processing of sensitive personal data will, however, require express consent (unless an exception exists).

Requirements for consent

The GDPR regulates that the controller must be able to demonstrate that the data subject gave his/her consent with processing their personal data. In other words, the burden of proof to demonstrate that the consent was given and that it was given validly is on the controller. The GDPR regulates in article 7 the formal and material conditions for the validity of the consent as follows:

- *Free manifestation of will, certainty, informedness, unambiguity:* the consent requires an unambiguous manifestation of will, which is a free, specific, informed and unambiguous expression of the data subject that he/she agrees with the processing of the personal data related to him/her.

  In order to ensure that consent is freely given, the controller should not rely on it if there is a clear imbalance between his and the data subject's position, in particular where the controller is a public authority and it is therefore unlikely that consent was given freely.

  Consent is not to be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

  For consent to be informed, the data subject should be aware of the fact and the extent to which consent is given, and at least of the identity of the controller and the purposes of the processing for which the personal data are intended.

- *Quoting separate purposes:* the consent must relate to all processing operations carried out for the respective purpose or purposes, and if the processing is carried out for more purposes, the consent should be given for, or should quote the respective purposes separately so that the data subject has an actual option to refuse granting consent for any of the purposes.

  Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case.

  In practice, "bundled" consents that combine several unrelated purposes will not be permissible.

- *Distinguishability, clarity, plain language:* if consent is given in the context of a written declaration, which also concerns other matters, the request for consent must be presented in a manner which is easily distinguishable from other matters, and it must be worded clearly and in plain language; an infringement of this provision may result in the consent being invalid.

  In practice this will mean that the part of the document containing the request for consent will have to be independent from e.g. other agreements, wording of orders, declarations, etc.

- *Intelligibility, accessibility:* the consent should be presented in an intelligible and easily accessible form, clearly and simply.

  This request may be particularly difficult to achieve, especially with regard to the extent of information the controller is obliged to provide to the data subject (the notification obligation will be discussed in a separate lesson).

- *Option to withdraw:* it must be as easy to withdraw consent as to give consent. Data subjects must be informed of the possibility to withdraw their consent prior to giving it.

In practice, businesses and institutions will be requested that they make the option to withdraw the consent accessible in the same way as it was given (e.g. through a web page, e-mail, privacy settings, etc.). The GDPR regulates that the withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal (i.e. prohibition of retroactivity), and the data subjects should be made aware of this fact prior to the consent.

- *Prohibition of inappropriate conditioning:* performance of a contract must not be made conditional on consent to the processing of personal data that is not necessary to perform the contract.

  When assessing whether consent is freely given, utmost account will be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent (e.g. performance of a purchase contract concluded on-line should not be made conditional to consent with the processing of personal data for marketing purposes). Otherwise there would be reasonable doubt to what extent the consent was given freely, and thus it's valid.

  Consent is presumed not to be freely given if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.

Recital 32 of the GDPR reads that consent may be given e.g. by a written statement, including by electronic means, or by an oral statement. Consent does not have to be express, but can include ticking a box when visiting an internet website (*opt-in*), choosing technical settings for information society services (e.g. by adjusting privacy settings on social media sites) or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent.

Consent for scientific research purposes

The GDPR admits that if personal data is to be processed for purposes of scientific research, it is often not possible to fully identify the purpose of personal data processing at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research. Data subjects should have the opportunity to give their consent only to certain areas of research or parts of research projects to the extent allowed by the intended purpose.

Consent with participating in scientific research within clinical studies will be regulated by a special Regulation[23].

Regarding the processing of children's personal data

In several occasions the GDPR regulates the specific conditions for processing children's personal data. In particular, recital 38 reads that children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Processing a child's personal data based on consent

The GDPR regulates the specific features of processing children's personal data based on consent as follows:

- if the controller processes personal data of a data subject based on his/her consent, in relation to the offer of information society services (e.g. social media) directly to a child,

[23] Regulation (EU) No. 536/2014 of the EP and of the Council from 16 April 2014 on clinical trials on medicinal products for human use.

the processing of the personal data of a child is lawful where the child is at least 16 years old[24];

- where the child is below the age of 16 years, such processing is lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child;
- the controller must 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.

These conditions relate to personal data collected through the internet, i.e. they do not relate to offline data. Also, they do not relate to processing personal data on a legal ground other than the consent. The above provisions will not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

The consent of the holder of parental responsibility will not be necessary in the context of preventive or counselling services offered directly to a child (such as help lines aimed at children).[25]

Other particularities related to processing of children's personal data

Children merit specific protection with regard to their personal data. Such protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

With regard to the above, any information and communication, where processing is addressed to a child, should be in such clear and plain language that the child can easily understand. The right to erasure and the "right to be forgotten" has a special meaning where consent was given during childhood where the data subject was not fully aware of all risks connected to the processing and later he/she desires to erase such data, especially on the internet.[26]

If the controller processes the personal data based on legitimate interest grounds[27], they must be able to demonstrate that they have responsibly and objectively assessed that the interests or fundamental rights and freedoms of the child whose personal data is processed do not override the legitimate interest pursued by the controller.

Pursuant to Article 40 (2) g) of the GDPR, associations and other bodies representing categories of controllers or processors may prepare codes of conduct for the purpose of specifying the application of this Regulation with regard to the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained.

Furthermore, each supervisory authority must, on its territory, promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing, whereby activities addressed specifically to children will receive specific attention.

What now

Controllers should ensure that they process personal data on relevant and legal grounds regulated by the GDPR. If personal data is processed based on consent, the formal and material conditions for consent, as well as the circumstances of its granting, should comply with the new legislation.

---

[24] Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.
[25] Recital 38, the last sentence, of the GDPR.
[26] Recital 65 of the GDPR.
[27] Article 6 (1) let. f) of the GDPR.

When processing personal data in relation to scientific research or in relation to children, additional conditions must be met.

Further information can be found here

Consent with processing personal data:

Recitals 32, 33, 40, 42, 43

Articles 6 sec. 1; 7

Processing children's personal data:

Recitals 38, 58, 65, 71

Articles 6, sec. 1; 8; 40 sec. 2; 57 sec. 1 let. b)

Lesson 5 of 16

Legitimate interest

Below you will learn:

Important changes

- When performing their tasks, public authorities will not be able to process personal data on the basis of "legitimate interest".
- Processors who process personal data based on "legitimate interest" should pay due attention to assess if a data subject's fundamental rights and freedoms do not prevail over the legitimate interest pursued by the controller.

Compliance Action Plan

If the controller processes the personal data based on legitimate interest, they should ensure that:

- The processing is also lawful after the GDPR comes into effect (please refer to Lesson 3 – Lawfulness of processing and further processing) and that this legal ground is relevant for the circumstances;
- for purposes of demonstrability, they keep record of how they assessed the data subjects' rights and freedoms that will be affected by the processing;
- data subjects are notified that their personal data will be processed based on this legal ground.

Regarding the specifics of "legitimate interest"

The GDPR regulates that the processing is lawful only when and to the extent that at least one of the stated conditions applies, whereby one of the conditions is that processing is necessary to serve 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 requiring the protection of personal data, in particular where the data subject is a child[28].

For the sake of comparison, the current Slovak legal regulation[29] (the "Slovak Act") stipulates that the controller may also processes personal data without the data subject's consent if processing the personal data is necessary to protect the legal rights and interests of the controller or the third party, mainly personal data processed in the scope of property protection, financial or other interests of the controller and personal data processed for the security purposes of the controller via video cameras or similar systems; this will not apply if fundamental rights and freedoms of data subject protected by this Act are predominant in such personal data processing.

Also, the current Czech legal regulation (the "Czech Act") stipulates that the controller may also process personal data without the data subject's consent if it is necessary to protect the legal rights and interests of the controller, receiver or another data subject. Such processing must not infringe the data subject's right to protection of their private and personal life[30].

The controller's protected interest (recognized by the legislation, not just by their own opinion) is proportionate to the protection of the right to privacy of the data subject (right to informational

[28] Article 6 (1) let. f) of the GDPR.
[29] Article 10(3) let. g) of Act no. 122/2013 Coll., the Data Protection Act as amended (Slovakia).
[30] Article 5 (2) let. e) of Act no. 101/2000 Coll., the Data Protection Act as amended (Czech Republic).

self-determination as a guaranteed fundamental right and freedom of the individual.[31] In case of a collision of these two interests/rights, it is necessary to assess if the controller's right prevails in a particular situation (or of the receiver or a data subject) or if it is the data subject's right to privacy that prevails. In other words, it is necessary to assess which interest has a higher value from the legal or social aspect. European courts and the Czech Constitutional Court decide this matter using a three-level proportionality test.[32]

Compared to the current legislation, the wording of the GDPR is broader and differs in the following:

- whereas the Act legitimizes the processing of personal data without the data subject's consent for the purpose of the *protection of rights and interests protected by law* of the controller or a third party, the GDPR states that personal data may be processed without the data subject's consent if it is necessary to serve the legitimate interests pursued by the controller or by a third party.

  This means that the exception from the obligation to have the data subject's consent regulated by the GDPR is broader than that regulated by the Act and can cover more processing operations.

  Whereas under the current legislation the condition of processing personal data *for the protection of rights and interests protected by law* must be met (i.e. there must be the explicit intention to protect the controller's or a third party's rights and interests) the GDPR does not regulate such condition. On the contrary, pursuant to the GDPR, it is sufficient if personal data is processed for the legitimate interests of the controller or a third party, without the protective factor.

  The new concept of legitimate interest will cover e.g. processing of personal data for marketing purposes or a one-off entry into a building, which purposes do not have an explicit protective character.

- As opposed to the current legal regulation, the GDPR regulates that the assessment of the balance of the legitimate interest pursued by the controller and rights and freedoms of data subjects who will be affected by the processing was carried out with a special consideration towards children[33].

  The GDPR aims for higher protection of children's rights and freedoms because they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. The GDPR obliges the controller to carefully document how and with what outcome the assessment of the balance of the controller's (or third party's) legitimate interest against a child's rights and freedoms was made.

  For purposes of assessment, if a data subject's (not just children's) rights and freedoms do not override the legitimate interest of the controller, it is necessary to take into consideration the reasonable expectations of data subjects based on their relationship with the controller. The existence of the legitimate interest requires careful assessment, including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could, in particular, override the

[31] Art. 10 (3) of the Charter of Fundamental Rights and Freedoms, Publish by the decision of the presidency of the Czech National Council no. 2/1993 Coll.; Art. 8 Charter of Fundamental Rights of the European Union; Art. 8 of Convention for the Protection of Human Rights and Fundamental Freedoms.

[32] I.e.: *1.* if the limitation is regulated by the law *2.* if the infringement is necessary and corresponds with the pursued legitimate interest. Refer to e.g. decision of the Constitutional Court of the Czech Republic file no. I.ÚS 321/06 dated 18 December 2006, decision of the plenum of the Constitutional Court of the CR file no. Pl. ÚS 4/94 dated 12 October 1994, and others. The usage of this test refers to e.g. the decision of the CJ EU dated 20 May 2003, in matters C-465/00, C-38/01 and C-139/01, *Österreichischer Rundfunk*; decision of the CJ EU dated 9 November 2010, in matters C-92/09 and C-93/09, *Volker und Markus Schecke GbR and Hartmut Eifert v. Hessen*.

[33] Please refer to Lesson 3.

interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing.

- Finally, the GDPR specifically states that public authorities will not be able to rely on the legitimate interest when carrying out their tasks. For this purpose, it will be necessary to consider the application of another legal ground[34].

Legitimate interest

The GDPR introduces the following examples of what types of processing could fall under the "legitimate interest" criteria:

- preventing fraud;
- direct marketing;
- if the controller is a part of a group of undertakings or institutions affiliated to a central body that may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data;
- preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems;
- indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data on public security to a competent authority.

The purpose of processing, including the legitimate interest, should be duly notified to the data subject prior to the commencement of the processing (the notification obligation will be discussed in a separate lesson).

Further the GDPR explicitly states[35] that the associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to the legitimate interests pursued by controllers in specific contexts. The controllers should verify if such a Code of Conduct exists that would regulate the processing operations they carry out.

What now

The controller should ensure that if they process personal data based on the legitimate interest pursued by them or a third party, data subjects' rights and freedoms do not override the legitimate interest, especially if the data subject is a child. Also, it is necessary to ensure that the controller is able to demonstrate how they assessed the balance of the legitimate interest against the data subjects' rights and freedoms.

Further information can be found here:

Recitals 47 - 50

Articles 6(1) let. f), 13(1) let. d), 14(2) let b), 40(2) let. b)

[34] E.g. Article 6(1) let. c) or e) of the GDPR.
[35] Art. 40(2) let. b) of the GDPR.

Lesson 6 of 16

Special category of personal data

Below you will learn:

Important changes

- The GDPR explicitly regulates that the term special category of personal data (after this "sensitive data") also contains genetic data and biometric data, if they are processed for unique identification of a person;
- The legal grounds for processing of sensitive data are slightly different from the current legal regulation;
- Member States are entitled to adopt their own modifications of processing sensitive data.

Compliance Action Plan

- If the controller process sensitive data, it is essential to correctly define the legal grounds of the processing;
- If the legal ground is the data subject's consent, it is necessary that it meets specific qualitative requirements.

Processing the special category of personal data

The GDPR defines sensitive data first as personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of a person. Also, the GDPR considers sensitive data genetic data[36], biometric data[37] for the purpose of uniquely identifying a natural person, data concerning health[38] or data concerning a natural person's sex life or sexual orientation.

The GDPR recognizes that sensitive data merit specific protection as the context of their processing could create significant risks to the data subject's fundamental rights and freedoms. Therefore, in Article 9 (1) the GDPR enshrines a general prohibition of its processing, which can only be overridden by the circumstances outlined in Article 9 (2). The possibility to override the general prohibition of processing sensitive data is regulated by an exhaustive list of exceptions; therefore, the circumstances under which it is possible to circumvent the general ban of processing sensitive data may not be extended.

Exceptions from the general prohibition of processing sensitive data

The general prohibition against processing sensitive data will not apply if one of the following conditions exist:

a) *the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition may not be lifted by the data subject;*

[36] Personal data relating to the inherited or acquired genetic characteristics of a natural person that give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
[37] Personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.
[38] Personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

Regarding the requirements for the granting of consent to be valid please refer to Lesson 4. However, please note the particularity regarding the consent for processing sensitive data, the consent must be explicit (a condition that does not apply if sensitive data is not processed).

Sensitive data cannot be processed where the applicable law states that even the data subject's explicit consent cannot override the general prohibition of processing sensitive data.

b) *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 in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;*

This legal ground extends the current regulation by explicitly stating that the processing of sensitive data is lawful where it is necessary to perform obligations arising from a collective agreement.

Processing personal data for purposes of employment law, social insurance and social security is possible based on the current legal regulation.[39]

c) *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;*

A comparable legal ground is contained in the current legislation. [40]

d) *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 and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;*

A comparable legal ground is contained in the current legislation.[41]

e) *processing relates to personal data which are manifestly made public by the data subject;*

and

f) *processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;*

A comparable legal ground is contained in the current legislation.[42]

g) *processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;*

This is an extension and further specification of the legal ground regulated in Article 14 let. b) of the Slovak Data Protection Act. Such legal ground is not yet regulated in the Czech legislation.

---

[39] Article 9 let. d) and f) of the Czech Data Protection Act no. 101/2000 Coll. and Article 14 let. g) of the Slovak Data Protection Act no. 122/2013 Coll.

[40] Article 9 let. b) of the Czech Data Protection Act no. 101/2000 Coll. and Article 14 let. c) of the Slovak Data Protection Act no. 122/2013 Coll.

[41] Article 9 let. e) of the Czech Data Protection Act no. 101/2000 Coll. and Article 14 let. d) of the Slovak Data Protection Act no. 122/2013 Coll.

[42] Article 9 let. g) and h) of the Czech Data Protection Act and Article 14 let. e) of the Slovak Data Protection Act no. 122/2013 Coll.

h) *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 on the basis of Union or Member State law or pursuant to contract with a health professional;*

and

i) *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, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;*

These two provisions extend and further specify the current legal ground regulated in the current legislation.[43]

Sensitive data may be processed for the purposes referred to in point (h) when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by competent national bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by competent national bodies.

j) *processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law, which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.*

It is a new provision under which the processing of sensitive data for the specified purposes is lawful if it is not inadequate in regard to the data subject's rights and appropriate safeguards for their protection are ensured (e.g. data minimisation, pseudonymization, etc.; please refer to Lesson 3).

Member States are entitled to maintain or introduce further conditions, including limitations, in regard to the processing of genetic data, biometric data or data concerning health. In regard to this provision, there may be further divergences in the conditions for processing this data in the legislation of various Member States, therefore entities processing such data on a cross border basis should pay due attention to existing nuances.

Changes in processing sensitive data

In connection to processing sensitive data the controller's obligations will change as follows:

- under Slovak conditions it is a novelty that the processing of a data subject's photograph or a graphic image of his/her signature will not be regarded as processing sensitive data, if they are not processed as biometric data, i.e. for a person's unique identification or authentication (e.g. for purposes of biometric passports);
- on the other hand, under Czech conditions, in the opinion of the Czech Office for Personal Data Protection[44], it is clear that portraits reflect the racial or ethnic origin of the depicted person, clothing or headgear may reflect the religion etc. A photograph or other image of the person is a document of a personal nature, which also includes biometric and other characteristics of the data subject, revealing the facts defined in Article 4 let. b) of the Czech Data Protection Act as sensitive data, and can therefore be a source of information for the processing of sensitive data. However, if the information from the photography of

[43] Article 9 let. c) of the Czech Data Protection Act and Article 14 let. f) of the Slovak Data Protection Act no. 122/2013 Coll.
[44] Opinion no. 12/2012, on the use of photography, video and audio recording of individuals.

the data subject is used for a mere distinction of its appearance compared to other persons and such information is not processed further, such use can't be considered as processing sensitive personal data. A similar view is also held by the Working Party WP 29, which in its opinion on online social networks notes that "*the working party in general does not consider images on the Internet as sensitive data, unless the images are clearly used to reveal sensitive data about individuals*."

- the controller will not have to notify the Data Protection Authority or be subject to the obligation to register pursuant to Article 33 of the Act[45], instead he/she will be required to keep records pursuant to Article 30 of the GDPR;
- if sensitive data is processed on a large scale[46], the controller will be obligated to carry out a data protection impact assessment and to appoint a data protection officer;
- the transfer of sensitive data to a third party with a seat in a third country which does not ensure an adequate level of protection of personal data will be lawful only based on the data subject's prior explicit consent, unless special legislation provides otherwise.

Criminal records / data on offences

The GDPR does not classify this information as sensitive data. It will continue to apply that the controller, for purposes of processing personal data relating to:

- criminal convictions and offences or related security measures; or
- processing personal data in criminal registers pursuant to a special legislation;

may be a relevant public authority empowered by law.

Any comprehensive register of criminal convictions will be kept only under the control of an official authority.

Processing of a national identification number

Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application (e.g. a birth number). In that case, the national identification number or any other identifier of general application may be used only with appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

What now

If the controller processes sensitive data, it is necessary to ensure that they do so based on a relevant legal ground pursuant to the GDPR. Should the legal ground be the data subject's consent, the wording and the way the consent is granted should be revised and updated in line with the new conditions.

Further information can be found here:

Recitals 51 – 56, 91, 97

Articles 4 (13) – (15), 9, 10, 87

[45] The Czech Data Protection Act no. 101/2000 Coll. and the Slovak Data Protection Act no. 122/2013 Coll., both as amended.

[46] The term "on large scale" is not defined in the GDPR and with regard to direct applicability of the GDPR, the Slovak Data Protection Authority is not entitled to propose a definition of this term into local legislation. Until the Working Party 29 introduces guidelines in relation to the interpretation of this term, controllers may refer to recitals 91 and 97 of the GDPR.

Lesson 7 of 16

Controller's obligation to inform data subjects

Below you will learn:

Important changes

- The GDPR regulates in more detail the extent of information that must be provided to data subjects;
- The GDPR emphasizes the requirement of clarity and intelligibility of the information provided to data subjects.

Compliance Action Plan

Controllers should:

- review existing data protection notifications and ensure that the wording complies with the GDPR;
- demonstrably notify data subjects of information required by the GDPR;
- ensure that the notification is carried out on time, comprehensibly and intelligibly.

In relation to the controller's obligation to notify data subjects

One of the fundamental principles of processing personal data is the principle of transparency. Therefore, the GDPR imposes an obligation on controllers to take appropriate measures to provide any information relating to the processing to the data subject, the extent of which the GDPR outlines.

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. If such information is to be provided to the public, it may be given in electronic form, for example, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose, personal data relating to him or her are being collected, such as in the case of online advertising.

The information obligation is fairly broad, whereby the legal framework for providing information to data subjects is as follows[47]:

- information must be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- information can be given in writing, electronically or my other means, or verbally upon request;
- information must be provided to the data subject free of charge. However, in case of unfounded or excessive requests by a data subject, the controller may charge a reasonable fee or refuse to act on the request (but bears the burden of demonstrating that the request is unfounded or excessive);
- the controller is entitled to request additional information necessary to confirm the data subject's identity;

[47] Article 12 of the GDPR.

- certain information may be provided in combination with standardized icons, which the Commission may introduce by means of delegated acts and the use of which will be shaped by later practice.

What information must be provided?

In comparison to the current Czech[48] and Slovak[49] legal regulation, controllers will also be obligated to provide data subjects with the following information[50]:

- contact details[51] of the controller, the controller's proxy, and the data protection officer, if he/she is appointed;
- legal grounds for the processing, and if the processing is based on Article 6 (1) letter f)[52] of the GDPR, also the legitimate interests pursued by the controller or by a third party;
- the period for which the personal data will be stored, or the criteria used to determine that period;
- information about 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;
- specification of the data subject's rights (for completeness we provide the complete list of the data subject's rights regulated by the GDPR, not just the new ones):
    - right to request from the controller access to his/her personal data;
    - right to rectification, completion, erasure or restriction of processing personal data;
    - right to object to processing;
    - right to portability of personal data;
    - the right to withdraw consent at any time if the processing occurs based on consent;
    - right to lodge a complaint with a supervisory authority;
    - right to know the existence of automated decision-making, including profiling.

Under Slovak conditions (this does not apply to the Czech Republic), processors will no longer need to inform data subjects about the processor by the processor and about the form of publication, if personal data was to be made public.

Further, under Slovak conditions the GDPR changes the current Slovak legal regulation[53] so that if the controller obtains personal data directly from the data subject based on the legal grounds of a

[48] Article 12 of the Data Protection Act no. 101/2000 Coll., regulating data subject's access to information about the purpose of processing personal data, personal data which are subject of processing, the recipients, etc.

[49] Article 15(1) of the Data Protection Act no. 122/2013 Coll., regulating the obligation to provide information about the identity and contact details of the controller and their proxy, if existing, purposes of processing, recipients and transfer of personal data to third countries.

[50] Article 13 and 14 of the GDPR.

[51] So far the law regulated the obligation to provide information about the "identity" (please refer to Article 10 let. a), Article 11 first indent of the Directive) in the Czech Act transposed as "who" (article 11(1)), in the Slovak Act transposed as "identification data" (article 15(1) let. a)). The legal literature explains the identification of the controller or processor as the obligation to provide a legal person's business name, ID no. and address, and a natural person's name, surname and place of residence or business.

[52] "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."

[53] Article 15(3) of the Data Protection Act no. 122/2013 Coll.

special law, international treaty or directly enforceable Act of the EU (in practice this will concern obtaining personal data for employment purposes) he/she will be obligated to provide the above-mentioned information to the data subject. The current legal regulation contains an exception, where in such cases notifications are not required, and this exception will not apply under the GDPR.

When should information be provided?

If the controller collects personal data directly from the data subject, he/she notifies him/her when the personal data is obtained[54].

If the controller does not obtain personal data directly from the data subject, he/she provides the information:

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

In such case the controller is obliged to inform the data subject, among the matters described above, of the categories of personal data processed about him/her and from which source the personal data originates, and if applicable, whether it came from publicly accessible sources.

Exceptions from the information obligation

The controller does not have to inform the data subject, if:

- the data subject already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort, or in so far as the information obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller must take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;
- obtaining or disclosure is expressly laid down by Union or Member State law, to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests[55]; or

---

[54] Pursuant to the Czech Act, this should occur when collecting data, i.e. at the latest when the controller requests data from the data subject. However, expert opinions deem the only acceptable interpretation that reflects the aim of the provision, the one that states that the data subject must be informed prior to the collection of personal data (compare e.g. Kučerová, A., Nováková, L., Foldová, V., Nonnemann, F., Pospíšil, D.: Data Protection Act. Commentary. 1st edition. Prague: C. H. Beck, 2012, s. 211).

[55] An exemption is regulated in Article 3(6) of the Czech Act in connection to ensuring security and defence of the State, of the public order, in connection to prevention, investigation, discovering of crimes and punishing crimes, important economic or financial interest of the Czech Republic and the EU or in connection to accessing files of former State Secret Services, and then in Article 11 (3) let. b) of the Czech Act, where it is regulated by a special Act (e.g. Act no. 372/2011 Coll., on Health Services) or data is necessary in relation to lodging claims and obligations of the controller arising from a special Act. Entities carrying out activities pursuant to special Acts are not exempt from the applicability of the Act as such, but they are exempt from the obligations regulating the basic parameters of data processing and obligations in relation to data subjects, such as the information obligation and the obligations relating to the data subject's access to his/her personal data. By means of an example, most activities of the Police corps would be difficult to realize under the application of the obligation to inform a person immediately about the collection of their data, or based on his/her request to fully disclose the processed personal data.

- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy; as well as
- if the GDPR does not apply to the processing of personal data, i.e.:
    - the processing is carried out by Member States in connection to activities related to common foreign and security policy pursuant to Title V, Chapter 2 of the Treaty on EU;
    - respective bodies for purposes of prevention, investigation, discovering or prosecuting of crimes or the execution of punishment, including prevention from threats for public security and their prevention, see Directive of the EP and of the Council (EU) 2016/680 dated 37 April 2016.

Further processing

If the controller intends to further process the personal data for a purpose other than that for which the personal data was obtained, the controller must provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as described above. (For more information on the lawfulness of further processing please refer to Lesson 3.)

What now

The information obligation of controllers to data subjects reflects one of the fundamental principles of processing personal data, which is the principle of transparency. To ensure transparency of processing it is necessary that the controllers inform data subjects about the circumstances of the processing in an intelligible and comprehensible manner. The extent of the information obligation is regulated by the GDPR. It might be a challenge to combine the obligation to provide a quite extensive amount of information with the request that the information should be concise.

In our opinion the future may bring certain interpretation challenges in connection to the provision regulating the information obligation, since the respective obligations and exemptions for certain types of processing or controllers are not regulated unambiguously in an absolute sense and their application could be somewhat obscure.

Further information can be found here:

Recitals 58, 60 – 63

Articles 12 – 14

Lesson 8 of 16

Data subject's rights (Part 1)

Below you will learn:

Important changes

Controllers will be obligated to:

- acquaint themselves with the content of data subject's new rights granted to them by the GDPR;
- implement effective internal procedures for handling data subject's requests concerning the processing (e.g. the duty to provide them with a copy of the data subject's personal data that they process and to demonstrate the lawfulness of processing);
- prepare policies and materials informing data subjects of how they can exercise their rights regarding the controller.

Data subjects can *inter alia* request:

- erasing their personal data if the processing is not lawful or if they withdraw their consent with processing;
    - if the controller made the processed personal data public (e.g. in connection with social media), if there is a grounded request for erasure, he/she is obligated to forward the request to all who process the published data. This obligation is formulated very broadly and its practical application will probably be a matter of further testing;
- restriction of processing his/her data, e.g. during the processing of their complaint related to the processing of their personal data or if the data subject objects against erasure for another reason.

Compliance Action Plan

Controllers should:

- create internal procedures for the timely handling of data subject's requests concerning the lawfulness of processing of their personal data (especially clients and employees);
- train a team of employees who handle the requests as to their rights and obligations;
- prepare template responses to requests, create procedures ensuring compliance with statutory periods, ensure that the data subjects are provided with all information to which they are entitled;
- ensure that the way of handling the requests meets the technical requirements of the GDPR;
- verify whether, in connection with the information obligation, another person's right to privacy will not be violated and create procedures for mitigating such risks;
- ensure that it is possible from the technical and organizational perspective to satisfy a request for erasure or restriction of processing in the controller's systems.

Regarding the data subject's rights

The GDPR extends and specifies the data subject's rights. For completeness we will include the list of all the data subject's rights as introduced by Chapter III of the GDPR. With regard to the extent of the matter we will discuss the data subject's rights in the next two lessons.

Right of access to personal data

In contrast to the controller's information obligation, as discussed in Lesson 7, the right of access to personal data is formulated differently: whereas the information obligation applies to the controller and obliges him/her to automatically, i.e. without a specific request of the data subject, provide the data subject with certain information, the right of access is independent from whether the controller met his/her information obligation, and entitles the data subject to access his/her personal data and to receive additional information about it on the basis of a his/her request.

The content of the right of access is the data subject's right to obtain from the controller confirmation as to whether or not personal data concerning him or her is being processed. If so, he/she is entitled to access (i.e. have a copy) to the personal data and receive further information[56] relating to the processing.

The controller must provide a copy of the personal data undergoing processing free of charge. For any further copies requested by the data subject, the controller may charge a reasonable fee reflecting administrative costs connected therewith. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information must be provided in a commonly used electronic form. This requirement is capable to induce further costs for entities processing personal data in paper form or in special formats, which will need to be converted into generally readable electronic form. Further costs can arise in connection to software and hardware equipment, administrative staff, etc.

Pursuant to Recital 63, the controller may provide remote access to a secure system, which would provide the data subject with direct access to his or her personal data. That means that if, e.g., the controller anticipates a greater frequency of data subject's requests for access to data, he/she may comply with this obligation by introducing a secure database of personal data into which the data subject will have access to the extent of his/her own personal data. However, this suggestion has a recommendatory rather than authoritative character.

The data subject's right of access to his/her personal data corresponds with the controller's obligation to implement internal procedures and organisational and technical measures in order to be able to satisfy the data subject's requests within a statutory period, which is "without undue delay" and in any event within one month of receipt of the request. This period may be extended by two further months where necessary.

Controllers should also introduce work procedures as to how to proceed in such occasions, train staff to process the requests, notify the staff of the obligations pertaining to data protection, e.g. about the obligation to maintain confidentiality, and to ensure that they have the appropriate technical and organisational equipment to be able to handle the data requests in a generally readable electronic format.

Exemptions from the right of access

The GDPR further regulates certain exemptions from the right of access to personal data:

- first of all, the right to obtain a copy of one's personal data must not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in

[56] I.e. a. the purposes of the processing; b. the categories of personal data concerned; c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period; e. 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; f. the right to lodge a complaint with a supervisory authority; g. where the personal data are not collected from the data subject, any available information as to their source; h. the existence of automated decision-making, including profiling, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject; i. where personal data is transferred to a third country or to an international organisation, the data subject has the right to be informed of the appropriate safeguards relating to the transfer.

particular the copyright protecting the software. Should the rights of another person be infringed by complying with the right of access to data, technical and organizational measures should be taken with the aim to avoid such infringement. However, the result of those considerations should not be a refusal to provide all information to the data subject. Since in this case there might be a collision of at least two equal rights or freedoms[57], in case of a dispute the respective court would be entitled to decide with final validity.

- where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates. However, this does not mean that if the processing of the data subject's request would be demanding as to the time and extent, that the controller would not be obliged to satisfy such request;
- the data subject's request should be motivated by verification of the lawfulness of the processing of his/her personal data; a request filed for a different purpose may not be satisfied by the controller.

The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

Right to rectification

The data subject has the right to have the controller, without undue delay, rectify inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject has a right to have incomplete personal data completed, including by means of providing a supplementary statement.

Right to erasure ("right to be forgotten")

The right to "be forgotten" raised many emotions during the legislative process of preparation the GDPR, especially in connection with providing information society services by companies such as Google, Facebook, etc. Services provided by these and other companies are specific in that they process an enormous amount of data subjects' personal data, store them on servers and further process them; with regard to the extensive amount of data and processing operations they anticipated many obstacles in regard to the right to be forgotten. This right, still governed only by case law[58] has, however, become a part of the GDPR's final wording, in the following content:

The data subject has the right to obtain from the controller the erasure of personal data concerning him or her without undue delay, if conditions regulated by the GDPR are met. This right corresponds with the controller's obligation to erase personal data 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;

  According to this assumption if personal data was collected or processed e.g. for the purpose of direct marketing, and the controller changed their business activities and no longer aims for marketing activities towards the data subject, his/her personal data should be erased.

[57] The data subject's right of access to personal data and another person's right e.g. to protection of personality, to privacy, privacy of correspondence, trade secret, IP rights, etc.

[58] At the EU level, see especially the judgment ECJ (Grand Chamber) of 13. 5. 2014, Case C 131/12 Google Spain SL, Google Inc. against the Agencia Española de Protección de Datos (AEPD), Mario González Costeja.

- the data subject withdraws the consent on which the processing is based[59], and where there is no other legal grounds for the processing;

  Withdrawal of the consent does not render the processing undertaken prior to the withdrawal unlawful. (Please refer to Lesson 4 for more information on consent).

- the data subject objects to the processing pursuant to Article 21(1) of the GDPR[60] and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2) of the GDPR [61];

  The right to object to processing will be discussed in the next lesson.

- the personal data have been unlawfully processed;

  This reason is very general and formulated so broadly that a large number of data subject's requests for erasure of data will be able to be included under it. The risk connected to it is that it will be the controller's obligation to demonstrate that data is processed lawfully (regarding the lawfulness of processing see Lesson 3). Thus, the fact that the data subject will claim that his/her personal data is processed unlawfully will be enough to shift the burden of demonstrating the opposite to the controller. The controller should therefore ensure that he/she is not in distress as to the evidence for proving the lawfulness of the processing, and to keep sufficient records about the processing and the legal grounds relating to it.

  It will be interesting to monitor how Member States will approach the implementation of exemptions[62] in their own legislation. Naturally, the controllers who process personal data on a cross border basis should acquaint themselves with these local specifics to ensure compliance of the processing in each Union State.

- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

  This applies e.g. to a situation where personal data processed so far should be erased after some time (and where an exemption allowing further processing, e.g. for archiving purposes in the public interest does not apply – see below).

- the personal data have been collected in relation to the offer of information society services referred to in Article 8(1) of the GDPR.

  That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child.

Specifics pertaining to published personal data

Where the controller has made the personal data public and is obliged to erase the personal data pursuant to the rules mentioned above, the controller will take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data

[59] Pursuant to Article 6 (1) let. a) or Article 9(2) let. a) of the GDPR.

[60] The data subject has a right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her if it 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 or if it 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 that require protection of personal data, in particular where the data subject is a child, including profiling based on those provisions.

[61] Where personal data is processed for direct marketing purposes, the data subject has the right to object at any time to the processing of his/her personal data, which includes profiling to the extent that it is related to such direct marketing.

[62] Article 23 of the GDPR.

subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. These measures will be taken taking into account the technology available and the cost of implementation.

This provision reflects perhaps one of the most revolutionary changes in the processing of personal data introduced by the GDPR. This provision basically obliges the controller who processed a data subject's personal data, and within this processing the data was made public, if the data subject submits a justified request for erasure of his/her personal data:

- to proactively adopt adequate measures including technical measures,
- to effectively inform controllers who process the said data that the data subject requests erasure of his/her personal data, its copies and replications,
- all of the above with regard to available technology and the cost of implementation.

Pursuant to Recital 66, the said measure was adopted specifically to strengthen the right to be forgottten in the online environment. However, it is not quite clear as to how the processor determines the group of controllers who process personal data that have been made public[63], and thus how to identify the concrete controllers whom the controller should notify of the request for erasing personal data. In practice, the application of this provision will be subject to further testing regarding how the compliance with this provision will be enforceable and to what extent the data subject's right reflecting this obligation will be eventually realisable.

Exemptions from the right to erasure

The above obligations of controllers will not apply if the processing is needed:

- for exercising the right to freedom of expression and information;
- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- for reasons of public interest in the area of public health[64];
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

Right to restriction of processing

Restriction of processing[65] means the controller is entitled only to store the personal data without any processing operations. If processing is done by automated means, it is necessary to adopt appropriate technical measures for this purpose (e.g. to withdraw it from the online environment). The data subject has a right to request that the controller restricts the processing if any of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

[63] For the sake of completeness, please note that in Slovak conditions after the GDPR becomes effective it will no longer be lawful to process personal data that has been made public pursuant to Article 10(3) let. e) of Act no. 122/2013 Coll. Pursuant to the GDPR, if no other legal grounds exist for processing of such data, the processing of data which was made public will be in contradiction to the principles of lawfulness, fairness and transparency, the principle of purpose limitation and compatibility of purposes.

[64] Pursuant to Article 9(2) let. h) and i) of the GDPR, and Article 9(3) of the GDPR.

[65] Article 4(3) of the GDPR.

- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pursuant to Article 21(1) of the GDPR pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted pursuant to the above rules, such personal data will, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

A data subject who has obtained restriction of processing will be informed by the controller before the restriction of processing is lifted.

Also

In connection to the right of rectification, erasure and restriction, the controller is obligated to communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed. This obligation does not apply if this proves impossible or involves disproportionate effort. The controller must inform the data subject about those recipients if the data subject requests it.

What now

In connection with the rights discussed above, the controller has extensive obligations to which we refer in the Compliance Action Plan section. To ensure compliance with the GDPR, controllers are advised to consult their legal advisors and IT professionals about their internal procedures for processing personal data.

Further information can be found here:

Recitals 63 - 69

Articles 15 - 19

Lesson 9 of 16

Data subject's rights (Part 2)

Below you will learn:

Important changes

- The right to data portability entitles the data subject to have the controller port his/her personal data directly to another controller;
- The content of the data subject's right to object to processing at the controller is changed; the data subject must be duly informed of this right;
- The data subject has a right not to be subject to a decision which:
    - is based solely on automated processing (including profiling); and
    - has legal effects on him/her or which similarly significantly affects him/her.

Compliance Action Plan

Controllers must:

- ensure that the processed personal data are easily portable in a structured, commonly used and machine-readable format;
- check that the data subject was duly informed of their right to object to processing at the time of the first communication;
- check if profiling is carried out and if yes, ensure that a relevant legal ground exists for it.

Right to data portability

The GDPR regulates the right to data portability as the data subject's right to:

- receive the personal data concerning him or her and subsequently have it transferred to another controller[66]; and to
- have the personal data transmitted by a controller directly to another controller.

In the first case, the right to receiving personal data can resemble the previously discussed *right of access to personal data* (refer to Lesson 8). The right to receiving the personal data is regulated more specifically with these differences:

- whereas the right of access to personal data entitles the data subject to access his/her data (i.e. *inter alia* to obtain a copy thereof) in a commonly used electronic form,
- the right to data portability is formulated narrower and in a more detail, in the sense that it entitles the data subject to obtain his/her personal data in a structured, commonly used and machine-readable format. From the technical aspect it is more specific and challenging for the controller, because he/she must provide the personal data in a structured, i.e. systematic and organized format[67].

The right to data portability may be exercised only if:

- the data was provided to the controller by the data subject;

[66] The exercise of this right is without prejudice to Article 17 of the GDPR regulating the right to erasure. Also, this right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

[67] Recital 68 also mentions an "interoperable format", but this is probably more of a recommendation than a binding character of the formulation.

- the processing is based on consent or explicit consent (in case of a special category of personal data), or it 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, and
- if the processing is carried out by automated means (i.e. not in paper form; for comparison – the right of access to personal data also pertains to data processed in paper form).

If the above conditions are not met, the data subject cannot invoke this right. For example, if the controller obtains the personal data from another controller and not directly from the data subject, the data subject would not have the right to data portability, only the right to access the data.[68]

If the data subject receives his/her personal data within the right to data portability, he/she is entitled to transfer it to another controller. However, this must not adversely affect the rights and freedoms of others. That means that should the right to data portability have a negative effect on the rights and freedoms of others, the transfer (or the provision of personal data to the data subject) should not occur. This situation could arise e.g. in the reality of social networks where among a data subject's personal data are also other people's personal data which is processed (e.g. within their mutual communication). In exercising the right to data portability, the rights of other persons must not be affected.

A significant change introduced by the new concept of the right to data portability lies in that the data subject can also request the controller not to transfer his/her personal data to him/her, but to transfer it directly to another controller. In practice this will be usable e.g. if the data subject can changes the provider of certain (e.g. telecommunication) services. The data subject would be deprived of the administrative and technical burden connected with the transfer of his/her personal data to another controller, whereas this obligation would pertain to the original data controller "in a structured, commonly used and machine-readable format". The only condition would be the technical feasibility of this request.

The right to object

The GDPR grants the right to object to the processing of personal data to the data subject only in certain specific cases. The data subject is not entitled to object to any processing, but only if:

1. the processing is necessary for:
    a. the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or
    b. the purposes of the legitimate interests pursued by the controller or by a third party;

    including objecting to profiling based on these provisions.

    In such cases the data subject is entitled to object to processing at any time, but only on "grounds relating to his or her particular situation". The burden of statement, why the processing should be ceased, is on the part of the data subject, who must state specific circumstances pertaining to his/her person or situation.

    If the data subject objected and stated relevant reasons, the controller must not continue the processing of such personal data, unless he/she demonstrates
        - compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject; or

[68] Such formalistic approach of the communitarian or other legislation does not have a material meaning in practical life. The data subject will be entitled / through the provision of the actual Czech Act (Article 12) and the Slovak Act (Article 15) – to the processed personal data, and not just to the information that their name, surname, date or birth, address, etc. is processed. Thus, there is no obstacle for the data subject to provide or to "transfer" the obtained personal data to another controller.

- reasons for the establishment, exercise or defence of legal claims.

  In such case the controller could continue the processing. That means that if the data subject files an objection based on the reasons above, the burden of proof shifts to the controller to demonstrate the existence of reasons that entitle him/her to continue processing the personal data for the stated purposes.

The data subject must be explicitly notified at the latest at the time of the first communication. This right must be presented clearly and separately from any other information.

2. processing for the purposes of direct marketing;

   The data subject is entitled at any time to object to the processing of his/her personal data for the purpose of direct marketing, including profiling in the extent to which it relates to it.

   It is an absolute right of the data subject, where he/she is not obliged to state or demonstrate anything else. In other words, if the data subjects does not wish that his/her personal data is processed for this purpose, it is sufficient that he/she objects at the controller who is obliged to cease the processing for this purpose immediately. The data subject is not obliged to state reasons pertaining to his/her special situation as in point 1 above. Also, there is no way for the controller could effectively oppose this objection (e.g. by means of claiming that his/her legitimate interest overrides the data subject's rights and interests). As soon as the data subject delivers the objection related to the processing of personal data for direct marketing purposes to the controller, the controller must not continue the processing for this purpose. If, however, the respective data is processed for a different reason based on a different legal ground, such processing is not affected.

   Similarly as in point 1, the controller must explicitly notify the data subject of this right, at the latest at the time of the first communication, and the right must be presented clearly and separately from other information.

3. processing for the purpose of scientific or historical research or for statistical purposes;

   If the personal data is processed for the above said purposes, the data subject can object to the processing based on grounds relating to his or her particular situation. He/she does not have this right if the processing is necessary for the performance of a task in the public interest.

   As in point 1, the data subject must state relevant reasons relating to his/her particular situation in order for the processing to cease.

   Contrary to objections pursuant to point 1 and 2, the data subject does not have to be notified of the right to object. The objection can also be raised by automated means using technical specifications.

Automated individual decision-making[69] and profiling[70]

[69] Automated individual decision-making is when a certain matter is decided by automated means, i.e. without any human intervention, e.g. based on certain algorithms defined in advance.

[70] Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements (Article 4(4) of the GDPR). Pursuant to Recital 71 of the GDPR the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect.

The GDPR provides data subjects protection against the risk of a potentially negative decision that was adopted without any human intervention, i.e. exclusively based on automated decision-making[71]. Recital 71 introduces an example of such decisions an automatic refusal of an online credit application or e-recruiting practices without any human intervention. The DGPR grants the data subject the right not to be affected by a decision which

- is based exclusively on automated processing, including profiling; and
- which has legal effects concerning him or her or similarly significantly affects him or her.

The protection against automated individual decision-making will not apply if the decision

a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

b) 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[72]; or

c) is based on the data subject's explicit consent.

In scenarios sub a) and c) the controller is obliged to introduce suitable measures for the protection of the data subject's rights. A minimum standard is to ensure the possibility of human intervention on the part of the controller, i.e. that the decision adopted by automated means will be reviewed by a person to enable the data subject to express his/her point of view to the circumstances of adoption of the decision and to contest the decision.

The automated decision-making must not be based on special categories of personal data (i.e. revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as in Article 9(1) of the GDPR), except in cases where it occurred based on

- explicit consent of the data subject, except where Union or Member State law provide that the prohibition may not be lifted by the data subject;
- substantial public interest, on the basis of Union or Member State law which is proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

  and where suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

What now

In order to ensure compliance with the GDPR in the extent of the right to data portability, right to object and rights connected to automated decision making and profiling, controllers should assure themselves to what extent they will be subject to this regulation (e.g. to what extent they will use profiling) and to correspondingly adjust internal processes pertaining to the processing and the communication with data subjects.

Also it will be essential to monitor further Union and local legislation, because the extent of rights and entitlements of data subjects, and the corresponding obligations of controllers, can be modified in favour of *inter alia* the protection of the data subjects or the rights of others, or with the aim to ensure the enforcement of civil claims.

[71] This is so far regulated in Art. 15 of the Directive, as a prohibition of decisions based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject, such as his/her performance at work, creditworthiness, reliability, conduct, etc. There is an exception for decisions taken in the course of the entering into or performance of a contract, lodged by the data subject, or if it is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests.

[72] E.g. for the purpose of tax-evasion monitoring and prevention conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller.

Further information can be found here:

Recitals 68 – 72

Articles 4(4), 20 – 23

Lesson 10 of 16

Security of personal data and personal data breach

Below you will learn:

Important changes

- Controllers will have a dual notification obligation in case of a personal data breach, i.e. towards the supervisory authority and towards the data subject;
- Controllers will be obliged to keep records of personal data breaches.

Compliance Action Plan

- Controllers and processors must implement appropriate security measures to protect the processed personal data;
- For this purpose it will be necessary to thoroughly review the circumstances of the processing in cooperation with IT technicians (e.g. for the purpose of implementing data encryption);
- Implementing internal policies in case a personal data breach is detected is recommended;
- Insurance for the consequences of a potential personal data breach is also recommended;
- Contracts with suppliers which contain the processing of personal data (e.g. payroll, accounting services) should contain provisions on liability for security of personal data[73].

Security of personal data

The GDPR sets out a minimum standard of personal data protection when processing, through several instruments or measures, which the controller is obliged to implement[74]. Considering the aim of the GDPR, it is clear that the main purpose of the new legislation regulating the processing of personal data is to ensure its security and minimize risks – not only from the consequences of human actions (intentional or by negligence, internal at the controller or the processor or external from other entities), but also natural causes or technical malfunction – related to various processing operations.

The GDPR regulates the controller's obligations connected with the security of personal data so that the controller (and processor) is obliged to implement appropriate technical and organisational measures with the aim to ensure an adequate level of security, including confidentiality, appropriate to this risk. These measures can include:

- the pseudonymisation and encryption of personal data;
- 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.

[73] Agreement on processing is considered a part of the security measures.

[74] These include, in particular, the obligation to keep records of processing activities, the obligation to implement appropriate technical and organizational measures, the obligation to notify the authority and data subjects of a personal data breach, impact assessment on the protection of personal data; previous consultations with the supervisory authority, etc.

The GDPR sets out the above mentioned security measures as examples, i.e. the controller may also determine other more suitable measures to ensure the security of the data pursuant to their specific conditions. The GDPR lays out the state that the controllers and processors should aim for, but not necessarily the measures. However, they must implement these measures taking into account:

- *the state of the art* – in order to ascertain what options for protecting personal data exist at the moment of determining the security measures, it is suitable that the controller consults the available means of protection with IT specialists. The measures must be of a certain professional level. It is recommended to review these on a regular basis; if during the processing of personal data the level of knowledge of the security measures increases, the controller might be in breach of the GDPR due to the obsoleteness of the security systems;
- *the costs of implementation* – when implementing specific measures the controller considers their costs. However, not implementing appropriate measures due to their financial, personal or time demanding character would not be a relevant argument;
- *the nature, scope, context and purposes of processing* – when determining what security measures the controller implements, he/she must thoroughly consider all circumstances of processing personal data at the time, when the processing is carried out. These circumstances must be reviewed from time to time with regard to the changing conditions of processing;

- risk of varying likelihood and severity for the rights and freedoms of natural persons – this is an important aspect of processing, whereby the controller is obliged to carry out an evaluation of any potential security risks connected to the processing, which may have a negative effect on the rights and freedoms of natural persons. This evaluation of risks should be carried out especially with regard to risks connected to automated processing (e.g. hacker attacks, IT malfunction, unauthorised or unprofessional interference of third persons into the processing) and with regard to risks connected to the environment in which the data is located (e.g. security of buildings and areas, fire prevention measures, accessibility of servers and other data storage rooms, etc.). When assessing the appropriate level of security, special consideration should be taken regarding the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed[75].

Which specific security measures the controller eventually implements should be a result of a detailed assessment of the circumstances of the processing in the conditions of the specific controller or processor.

A substantial change is introduced with the GDPR's effectiveness, being that controllers will no longer have to elaborate security projects[76] or security documentation[77] as previously required. Instead – where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons – the controller will have to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (*"privacy impact assessment", "PIA"*) prior to the processing, or to consult with the supervisory authority pursuant to Articles 35 and 36 of the GDPR. This obligation will apply in specific cases, e.g. with large scale systematic monitoring of publicly accessible areas, large scale processing of special categories of personal data or of personal data relating to criminal convictions and offences referred, profiling or automated decision making, etc.

[75] Article 32(2) of the GDPR.
[76] Article 20 of Act no. 122/2013 Coll., the Data Protection Act as amended (Slovak).
[77] Article 13 (2) of Act no. 101/2000 Coll., the Data Protection Act as amended (Czech).

For purposes of ensuring and demonstrating the implementation of security measures it is possible that the controller adheres to an approved code of conduct[78] or an approved certification mechanism[79]. Also, the controller must ensure that any natural person acting under the authority of the controller, who has access to personal data (currently a so called "entitled person"), processes it only based on the controller's instructions, unless he or she is required to do so by Union or Member State law.

A substantial obligation of the controller and processor will be the detailed supervision of the performance of the implemented measures and the data protection officer's obligations. The PIA or a consultation with the supervisory authority and the subsequent implementation of technical or organizational security measures will not be sufficient.[80]

Notification of a personal data breach

However responsibly the controller approaches the protection of personal data processed by them, the risk of a personal data breach will probably still not be completely mitigated. Such personal data breach may be an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed[81].

In relation to a personal data breach the GDPR regulates two types of the controller's notification obligation:

a) Notification of the personal data breach to the respective supervisory authority

In case of a personal data breach the controller is first of all obliged to notify the supervisory authority competent in accordance with Article 55 of the GDPR. This notification must be carried out without undue delay, but where feasible not later than 72 hours after having become aware of it. Where the notification is not made within the stated period, it must be accompanied by reasons for the delay.

Where and in so far as the controller cannot from objective reasons provide the supervisory authority the requested information at the same time, the information may be provided in several phrases without undue further delay.

The notification must at least:

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

The controller does not have to notify the supervisory authority if the personal data breach is unlikely to result in risks for the rights and freedoms of natural persons.

---

[78] Article 40 of the GDPR.

[79] Article 42 of the GDPR.

[80] The supervision does not have to be specifically data protection oriented; it can be a part of exercising the rights and duties of managing employees to supervise the work of subordinate employees within an employment relationship. It is also possible to use standard automated means, such as logs (recording of access of a specific person into a system).

[81] Article 32(2) of the GDPR.

b) Notification of the personal data breach to data subjects

If a personal data breach occurs which is likely to result in a high risk to the rights and freedoms of natural persons, the controller must communicate the personal data breach to the data subject. This communication must occur without undue delay.

In the communication to the data subject the controller states in clear and plain language the nature of the personal data breach and at least the following information and measures:

- the name and contact details of the data protection officer or other contact point where more information can be obtained;
- the likely consequences of the personal data breach;
- measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Also in this case the GDPR sets out an exception from the notification obligation. The communication to the data subject is not required if any of the following conditions are met:

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

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

Documenting personal data breaches

Among the above mentioned notification obligations the controller is obliged to internally document each occurrence of a personal data breach, including circumstances related to the breach, its effects and remedial action taken, and to maintain these records.

Also, the controller must keep a certain communication (i.e. documentation) standard in relation to the notification of the personal data breach to the supervisory authority and to the data subjects (please see above the requirements of such notifications).

What now

Prior to the GDPR's effectiveness, controllers and processors should review their current internal technical and organizational measures with regard to the new requirements, evaluate the risks with regard to the current state of the art, the costs of implementation and the nature of processed personal data, update their current security measures and supervisory and liability mechanisms and ensure due record keeping and procedures for a timely notification of potential security incidents. If they detect a high risk for the rights and freedoms of natural persons, a PIA should be undertaken or the Authority should be consulted. The controllers and processors should be able to demonstrate and justify these steps retroactively, to demonstrate and prove that they are not liable for potential damages under civil law (damage caused to a data subject), administrative law

(for an administrative tort) or criminal law (e.g. for the crime of unlawful handling of personal data).

Further information can be found here:

Recitals 83 - 94

Articles 32 – 34

Lesson 11 of 16

Codes of conduct and certification

Below you will learn:

Important changes

- The GDPR introduces new institutes for ensuring and demonstrating that the processing is in compliance with the GDPR, i.e.:
    - codes of conduct, and
    - certification mechanisms, seals and marks;
- Controllers and processors can ensure and maintain compliance with the GDPR through codes of conduct more easily;
- Adherence to codes of conduct will be monitored by accredited entities; if a breach of the code of conduct on the side of the controller or processor is discovered, they can be suspended from participation in the code;
- Certification mechanisms, seals and marks will be introduced for voluntary "self-regulation" by the controller or the processor;
- If the controller or processor adheres to some of these instruments, compliance with the GDPR will be demonstrated for a period of 3 years (the validity of the certification can also be extended).

Compliance Action Plan

Controllers and the processors should:

- monitor whether approved codes of conduct exist in their sector, valid within Slovakia or the EU;
- find out whether certifications, seals or marks exist, which they could obtain and so demonstrate compliance with the GDPR;
- learn about existing certificates, seals or marks, which will be introduced from time to time, and to take these instruments into account when choosing their processors or service providers.

Codes of conduct

The GDPR regulates codes of conduct as documents elaborated by associations or other bodies representing categories of controllers or processors, regulating the processing of personal data specific for these groups of controllers or processors. The codes should contribute to the proper application of the GDPR, taking account the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

The codes will be important for controllers and processors who, by adhering to them, will be able to easily and reliably ensure and demonstrate to the supervising authorities their compliance with the GDPR.

By undertaking to observe an approved code of conduct, the controller or the processor may benefit in several ways, such as:

- best practices will be developed through the codes, regulating how personal data is handled in the respective sector and in the specific context of processing;
- the controller or the processor may rely that the processing of personal data is done lawfully, which can e.g. save financial resources on professional advisors in this area;

- data subjects will consider participation in the approved code as a sign of credibility and assurance that their personal data is processed lawfully;
- together with an enforceable obligation of the data importer residing outside of the EU to adopt appropriate safeguards, approved codes may be used to ensure the lawfulness of the transfer of personal data outside the EU, similar to standard contractual clauses and binding corporate rules;
- compliance with the GDPR may be demonstrated to the supervisory authority more easily.

An association or other bodies representing categories of controllers or processors can prepare a code of conduct relevant for their sector or industry. The code should serve as a "manual" for companies operating in the respective sector, how to correctly carry out processing operations specific for their sector, e.g. entities operating in the banking sector, health and education, pharmaceutical industry, retail, IT sector including cloud services, etc.

The codes may regulate recommended procedures with regard to e.g.: fair and transparent processing, the legitimate interests pursued by controllers in specific contexts, the collection of personal data, the pseudonymisation of personal data, the information provided to the public and to data subjects, the exercise of the rights of data subjects, the information provided to, and the protection of, children, and the manner in which the consent of the holders of parental responsibility over children is to be obtained, the measures and procedures useful for adopting the appropriate technical and organisational measures and measures to implement data protection by design and by default, security measures, the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects, the transfer of personal data to third countries or international organisations, or out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects.

Approving codes

In order for a code of conduct to have the effects as explained above, it must be approved by a competent supervisory authority. The process of approval depends upon whether the code should be valid within a member state, or if it should have general validity within the Union.

If a code is does not relate to processing operations outside a certain member state (e.g. Czech Republic or Slovakia), its draft must be submitted to the respective supervisory authority (in this case the Czech or Slovak Data Protection Authority). The supervisory authority provides an opinion on whether the draft code complies with the GDPR and approves that draft code if it finds that it provides sufficient appropriate safeguards. That supervisory authority also registers and publishes the code.

On the other hand, where a draft code of conduct relates to processing activities in several Member States, the competent supervisory authority, before approving the draft code, submits it in the procedure of cooperation between supervisory authorities of the of the Union and of the Commission to the European Data Protection Board (the "Board"), which provides an opinion on whether the draft code complies with the GDPR or provides appropriate safeguards.

If the Board in its opinion confirms that the draft code complies with the GDPR, or provides appropriate safeguards, the Board submits its opinion to the European Commission. The Commission may, by way of implementing acts, decide that the approved code of conduct, as submitted to it is generally valid within the Union. The Commission ensures appropriate publicity for the approved codes which have general validity. The Board collates all approved codes of conduct in a register and will make them publicly available using appropriate means.

Monitoring compliance with codes of conduct

Besides the competent supervisory authority, compliance with codes of conduct can be monitored by a body which has an appropriate level of expertise and is accredited for this purpose by the competent supervisory authority. Such body must:

- demonstrate its independence and expertise in relation to the subject-matter of the code;
- establish procedures which allow it to assess the eligibility of controllers and processors concerned to apply the code, to monitor their compliance with its provisions and to periodically review its operation;
- establish procedures and structures to handle complaints about infringements of the code or the manner in which the code has been, or is being, implemented by a controller or processor, and to make those procedures and structures transparent to data subjects and the public; and
- demonstrate that its tasks and duties do not result in a conflict of interest.

The criteria for the accreditation will be determined by the respective supervisory authority after consulting with the European Data Protection Board. If the accredited body discovers non-compliance with the code, it can impose a sanction to the controller or the processor, in the form of appropriate measures, including suspension or exclusion of the controller or processor concerned from the code.

Certification

The GDPR regulates certification mechanisms, seals and marks as further instruments of protection of personal data. These mechanisms should increase the transparency of the processing, and should help data subjects to quickly assess the level of protection of personal data for relevant products and services. Such example is a situation when data protection seals or marks will be introduced for a certain service, e.g. providing of cloud services, which will mean that the entity who obtains them meets the GDPR's requirements for lawful processing[82].

Certification of processing personal data is an important milestone for creating a reliable and transparent framework for processing. These mechanisms can be implemented by Member States, the supervisory authorities, the Board and the Commission. They should be applied preferably at the Union level, but their validity in a local extent is also admissible. The specific needs of micro, small and medium-sized enterprises should be taken into account.

Certification is voluntary, but does not reduce the responsibility of the controller or the processor to comply with the GDPR. In other words, if e.g. the controller obtains certification, but violates the GDPR by a processing operation, the certification does not limit his liability. The certification can be issued for a maximum period of three years and may be renewed, under the same conditions. Similarly, if the conditions for certification cease to be met, certification can be withdrawn.

Certification may have the following benefits for controllers and processors:

- controllers and processors will be able to demonstrate compliance with the GDPR more easily, especially in connection to adopting appropriate technical and organisational measures;
- data subjects or clients who look for a service provider can take certification into account as a proof of credibility and expertise of the service provider of (e.g. cloud) services; and
- similar to codes, together with an enforceable obligation of the data importer residing outside the EU to adopt appropriate safeguards, certifications may be used to ensure the

[82] For better understanding the ISO certificate can be considered, which proves that the subject who obtained it, meets a certain quality in the respective area, as required by this certificate.

lawfulness of the transfer of personal data outside the EU, similar to standard contractual clauses and binding corporate rules.

Besides the supervisory authorities, the GDPR also gives the power to grant certifications to certification bodies, which are duly accredited for this activity. Under Slovak conditions the Slovak Data Protection Authority will be entitled to grant accreditation to certification bodies. To obtain accreditation of a certification body, the following criteria set by the GDPR must be met:

- demonstrating independence and expertise in relation to the subject-matter of the certification;
- undertaking to respect the criteria approved by the Board or the competent supervisory authority;
- establishing procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks;
- establishing procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and making those procedures and structures transparent to data subjects and the public; and
- demonstrating that the tasks and duties of the accreditation applicant do not result in a conflict of interest.

The accreditation of a certification body will be issued for a period of 5 years maximum with the option of renewal.

What now

Controllers and processors can benefit from participating in approved codes of conduct (valid either within a Member State or within the Union), or from data protection certifications, seals or marks which will be introduced after the GDPR becomes effective. Therefore it is recommended that controllers and processors monitor the implementation of these instruments to be able to decide if they will seek to participate in or obtain them.

Further information can be found here:

Recitals 77, 81, 98 – 100, 148, 166, 168

Articles 40 – 43, 57(1) let. p), q), (3) let. e), 64 (1) let. c), 70 (1) let. o), p)

Lesson 12 of 16

Transfer of personal data outside the EU/EEA

Below you will learn:

Important changes

- The requirements for the transfer of personal data will mostly concern international companies and companies which use services that entail the transfer of data to third countries (e.g. cloud services);
- In comparison to the previous legal regulation, new possibilities to ensure the lawfulness of data transfer outside the EU/EEA have been introduced.

Compliance Action Plan

Controllers and processors should:

- review the flow of processed personal data;
- if personal data is transferred outside the EU/EEA, check whether mechanisms for ensuring the lawfulness of the transfer (e.g. model clauses, binding corporate rules, etc.) are implemented;
- check if and where their service providers transfer the personal data received from them;
- if in the past the transfers occurred based on the "Safe Harbour", implement a different legal grounds for the transfer, since the Safe Harbour was abolished and is no longer valid.

Transfer of personal data outside the EU/EEA

Similar to the previous legal regulation, the GDPR also regulates the conditions of data transfer to third counties (outside the EU/EEA) and to international organisations[83]. The rationale for this is the fact that as soon as the personal data leaves the territory where EU law applies, it becomes subject to foreign laws which may not ensure an adequate protection of personal data on a level comparable with Union law. Therefore, this topic will be relevant mostly for international companies and companies which use the services of providers operating outside of the Union (e.g. if they use cloud services and servers located in third countries). On the contrary, this topic will not be relevant to companies who do not transfer data or transfer them only within the EU/EEA.

The starting point for understanding the need to regulate data transfers outside the EU is explained in Recital 101 of the GDPR, according to which flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data is transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by the GDPR should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation.

The transfer of personal data to third countries will be possible if any of the following conditions is met:

[83] Article 4 (26) of the GDPR: *an organisation and its subordinate bodies governed by public international law, or any other body which is set up by, or on the basis of, an agreement between two or more countries*.

Transfer on the basis of an adequacy decision

The European Commission (the "Commission") can decide that a third country, a territory or one or more specified sectors within that third country, or the international organisation ensures an adequate level of protection. Such a transfer does not require any specific authorisation[84]. At least every four years there must be a periodic review of the circumstances on the basis of which the Commission issued its decision.

If the Commission discovers that the circumstances impacting the protection of personal data in a third country (or an international organisation) have been negatively changed, it can decide that such country no longer ensures an adequate level of protection. Such decision does not have a retroactive effect, thus it is effective at the earliest on the day of its adoption. Therefore, the question remains regarding the security of the data that was already transferred.

The Commission will publish in the Official Journal of the European Union and on its website[85] a list of the third countries and international organisations for which it has decided that an adequate level of protection is or is no longer ensured. Currently, countries ensuring an adequate level of protection are: Andorra, Argentina, Canada, Switzerland, Faeroe Islands, Guernsey, Isle of Man and Jersey, Israel, New Zealand and Uruguay.

Transfer to the United States of America has certain specific features. Until 2015 transfer to the USA was possible *inter alia* based on the "Safe Harbour" scheme[86], which allowed for the transfer of personal data to entities located in the USA and registered within the Safe Harbour without additional measures and formalities. However, on 6 October 2015 the Grand Chamber of the CJ EU issued a decision[87], by which it abolished the respective Commission's decision regulating the Safe Harbour, and from this date the transfer of personal data to the USA based on this legislative act is no longer considered lawful[88].

This scheme was substituted by a so called "Privacy Shield"[89], which was passed by the Commission on 12 June 2016. The list of companies which bound themselves to comply with the principles of data protection implemented through the Privacy Shield is published on the US Department of Commerce's website[90].

Transfers requiring adequate safeguards

In the absence of a decision of the Commission as explained above, the transfer of personal data to a third country or an international organisation can be undertaken only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject

---

[84] When accessing the adequacy of the level of protection of personal data, the Commission takes into account elements: the rule of law, respect for human rights and fundamental freedoms, relevant legislation, as well as the implementation of such legislation, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization, effective administrative and judicial redress, the existence and effective functioning of independent supervisory authorities, international commitments, etc.

[85] http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[86] Decision of the Commission 2000/520/EC of 26 July 2000, which contained the principles and requirements related to the protection of personal data, to which entities residing in the USA could voluntarily submit themselves and so to be regarded as reliable when handling of personal data.

[87] http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0362&lang1=sk&lang2=EN&type=TXT&ancre=

[88] The basis for this was a petition of an Austrian citizen Max Schrems, who was a Facebook user from 2008. Facebook transferred personal data of its users to servers located in the USA, where it was further processed. Mr. Schrems filed a complaint with the supervisory authority in Ireland, the purpose of which was that pursuant to information revealed by Edward Snowden in 2013 in relation to the manner in which the American security agencies (especially NSA – National Security Agency) handle personal data in their jurisdiction (i.e. also data of European users), the USA do not ensure protection from surveillance from the side of American authorities. The Irish supervisory authority refused the complaint referring to the safeguards ensured by the American authorities through the Safe Harbour. Upon investigating the matter the CJ EU abolished the Safe Harbour scheme.

[89] http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

[90] https://www.privacyshield.gov/welcome

rights and effective legal remedies for data subjects are available. The appropriate safeguards may be provided for, without requiring any specific authorisation from a supervisory authority, by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules;

  In case of a group of companies, which has subsidiaries in the Union and in third countries, the transfer of personal data within this group of companies can also be carried out on the basis of binding corporate rules. In order for the rules to be binding, they must be approved by the competent supervisory authority, after which they are binding not only within the jurisdiction of the supervisory authority which approved them, but also in all other jurisdictions where the group has subsidiaries. The supervisory authority approves the rules, if:

  - they are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;
  - expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and
  - fulfil further requirements, e.g. the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members, the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question, their legally binding nature, both internally and externally, the rights of data subjects in regard to processing and the means to exercise those rights, the complaint procedures, cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, etc.
- standard data protection clauses adopted by the Commission or adopted by the supervisory authority and approved by the Commission; model clauses that were adopted prior to the GDPR remain valid[91];

  If the controllers or processors use standard contractual clauses for the transfer of data outside of the Union, they can include them in a wider contract, such as a contract between the processor and another processor, or add other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses or prejudice the fundamental rights or freedoms of the data subjects;
- an approved code of conduct (please refer to Lesson 11 for further information regarding this new instrument) together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or
- an approved certification mechanism (please refer to Lesson 11 for further information regarding this new instrument) together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Derogations

In the absence of an adequacy decision or of appropriate safeguards including binding corporate rules, a transfer of personal data to a third country or an international organisation can take place only on one of the following conditions:

- the data subject has explicitly consented to the proposed transfer;

[91] http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

The transfer to a third country or an international organization may take place if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject, and the controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. In such case the controller must inform the supervisory authority of the transfer.

What now

Controllers and processors should verify if they transfer personal data outside the EU/EEA, or if such transfers are realized by their suppliers of services or goods. Subsequently such transfers must be based on one of the valid legal grounds for the transfer, e.g. on basis of an adequacy decision or on basis of adequate safeguards. If the transfer cannot be grounded by one of the existing legal grounds, it is necessary to ascertain if the transfer can be subject to a derogation from this obligation.

Further information can be found here:

Recitals 6, 23, 101 - 116

Articles 44 – 49

Lesson 13 of 16

Supervision over processing personal data

Below you will learn:

Important changes

- In certain cases, controllers and processors may be subject to supervision of not only the supervisory authority of the state in which they are established, but of the supervisory authority of another Union member state, which will have the status of a lead authority;
- A new European Union body will be established – the European Data Protection Board.

Compliance Action Plan

Controllers and processors should:

- become familiar with the extensive powers of the supervisory bodies;
- if they carry out cross border processing, becoming familiar with the functioning and cooperation of the lead supervisory authority and local supervisory authorities is recommended.

Supervision over processing personal data

Supervising the processing personal data is another extensive chapter of the GDPR. According to Recital 117 of the GDPR, the establishment of supervisory authorities in Member States is an essential component of the protection of natural persons with regard to the processing of their personal data. The supervisory authorities' role is to monitor and eventually to authoritatively ensure compliance with the GDPR for purposes of protecting the rights and fundamental freedoms of the data subject whose personal data is processed.

In the area of supervision over processing personal data the GDPR introduces several new concepts and even a new EU institution, in which all Member States will be represented. It will be of essence for controllers and processors to become familiar with which supervisory bodies they will be subject to in the extent of which processing operations, and what obligations they will have towards these authorities.

Local supervisory authorities

First of all, controllers and processors will be subject to the supervisory authority of the state in which the controller is established (for ease of reference we will refer to such DPA as the "local supervisory authority", although the GDPR does not use this term). In Slovak conditions this would be the Data Protection Office of the SR[92], in Czech conditions the Data Protection Office of the CR[93].

The local supervisory authority is competent to supervise processing:

- in the context of the activities of a controller or processor established on its own Member State territory.

  The local supervisory authority will not be automatically competent to carry out supervision over cross border processing of personal data within two or more member states (for such processing please refer to the "*Lead supervisory authority*" below), but only over

[92] Website: https://dataprotection.gov.sk/uoou/ .
[93] Website: https://www.uoou.cz/ .

processing operations carried out within one state (also when it is carried out by a controller or processor who otherwise conducts cross border processing);

- carried out by public authorities or private bodies acting in the public interest.

  Typically these are processing operations of State administrative bodies and self-administration bodies. Supervisory authorities are, however, not competent to supervise processing operations of courts acting in their judicial capacity;

- affecting data subjects on its territory.

  The local supervisory authority will always be competent if rights of data subjects located in its own territory are in question, i.e. regardless whether it is a local or cross border processing (this is an exception from the rule explained in the first bullet point above). The local supervisory authority is always competent to handle a complaint lodged with it or a possible infringement of the GDPR if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State;

- carried out by a controller or processor not established in the Union when targeting data subjects residing on its territory.

  This type of a supervisory power relates to the extended applicability of the GDPR (please refer to Lesson 1). This means that the local supervisory body will have competence over e.g. a Chinese controller which is not established in the EU, but which offers goods or services in a Member State.

Lead supervisory authority

If the controller or the processor process personal data on a cross border basis (whether through one or more establishments in the Union), it will also fall under the lead supervisory authority which is competent as the main supervisory authority for cross border processing. Processing operations which do not contain a cross border element will continue to fall under the local supervisory authorities; however, in case of cross border processing, the lead supervisory authority will be competent.

All (also other than lead) supervisory authorities will be competent to handle a complaint lodged with it or a possible infringement of the GDPR if the subject matter relates only to an establishment in its Member State or substantially affects data subjects only in its Member State. Also in case of cross border processing, any supervisory authority may act under said conditions. However, the supervisory authority must first notify the lead supervisory authority, which decides if it will deal with the case or not.

If the lead supervisory authority decides that it will not deal with the matter, the local supervisory authority will be competent. If the lead supervisory authority decides that it will deal with the matter, the supervisory authority who notified the lead supervisory authority can deliver a draft decision to the lead supervisory authority, which will subsequently follow the cooperation procedure.

Cooperation between the lead supervisory authority and the other supervisory authorities concerned

- *Cooperation and exchange of information:* the lead supervisory authority cooperates with the other supervisory authorities concerned in an endeavour to reach consensus. The lead supervisory authority and the supervisory authorities concerned exchange all relevant information with each other.
- *Submitting a draft decision to other supervisory authorities of opinion:* the lead supervisory authority without delay communicates the relevant information on the matter to the other

supervisory authorities concerned. Without delay it submits a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views.

  - *Submitting the matter to the Board:* where any of the other supervisory authorities concerned within a period of four weeks expresses a relevant and reasoned objection to the draft decision, the lead supervisory authority, if it does not follow such objection or is of the opinion that it is not relevant or reasoned, submits the matter to the European Data Protection Board (the "Board").
  - *Submitting a revised draft of the decision for opinion to other supervisory authorities concerned:* where the lead supervisory authority intends to follow the relevant and reasoned objection made, it submits to the other supervisory authorities concerned a revised draft decision for their opinion.

- *Adopting a decision:* the lead supervisory authority adopts and notifies the decision to the main establishment or single establishment of the controller or processor, as the case may be, and informs the other supervisory authorities concerned and the Board of the decision in question, including a summary of the relevant facts and grounds. The supervisory authority with which a complaint has been lodged informs the complainant of the decision. Where a complaint is dismissed or rejected, the supervisory authority with which the complaint was lodged adopts the decision and notifies it to the complainant and informs the controller thereof.
- *Ensuring compliance:* the lead supervisory authority ensures that the controller or processor take the necessary measures to ensure compliance with the decision as regards processing activities in the context of *all* its establishments in the Union. The controller or processor notifies the measures taken for complying with the decision to the lead supervisory authority, which informs the other supervisory authorities concerned.

The rules for determining the lead supervisory board of the controllers or processors, including a broader discussion on the topic with practical examples, is contained in the document drafted by WP 29.[94]

European Data Protection Board

The GDPR regulates a new independent body of the Union with its own legal personality – the European Data Protection Board (the "Board"). The board is a body of the European Union and is created from the representatives of supervisory authorities of all Member States and the European Data Protection Supervisor.

Although the controllers and the processors will not be directly subject to the supervision of the Board, the Board may have impact on the processing of personal data. The Board has a list of duties, among which it ensures a consistent application of the GDPR. For this purpose and in the context of the mechanism of consistency, it cooperates with supervisory bodies of the Member States when adopting decisions.

What now

For controllers and processors which process personal data only within one jurisdiction, only the supervisory authority in that particular member state will be relevant. However, if you process personal data on a cross border basis, it will be essential to realize that these processing operations may be subject to the supervision of the lead supervisory authority. Controllers and processors should be prepared to communicate with other than their local supervisory authority.

---

[94] Guidelines for identifying a controller or processor´s lead supervisory authority; adopted by the Article 29 Data Protection Working Party on 13 December 2016, revised on 5 April 2017, WP 244 rev. 01.

Further information can be found here:

Recitals 117 – 140

Chapters VI and VII

Lesson 14 of 16

Remedies

Below you will learn:

Important changes

Data subjects (and in some cases also other persons, e.g. controllers) have the following remedies at their disposal:

- Right to lodge a complaint with a supervisory authority;
- Right to an effective judicial remedy against a supervisory authority;
- Right to an effective judicial remedy against a controller or processor;
- Right to compensation for material or non-material damage.

Compliance Action Plan

- Controllers and processors should by means of effective contractual measures mutually and in detail define the extent of their obligations, the sanctions for their breach, how to resolve disputes and liabilities involving data subjects.
- Joint controllers should agree on the extent of their obligations in order to reach compliance with the GDPR, the extent of liability for breach of the GDPR, how to resolve disputes and the method of carrying the liability for damage.

In relation to remedies

Right to lodge a complaint with a supervisory authority

In the first place, the GDPR grants data subjects the right to lodge a complaint with a supervisory authority, if he/she believes that the processing of his/her personal data violates the GDPR. The purpose of this legal instrument is to protect the rights the GDPR grants data subjects when facing violations by controllers or processors.

As mentioned in Lesson 13, the processing operations of the controller can be subject to the supervision of at least two supervisory authorities, i.e. the authority competent pursuant to the place of the controller's registration or the lead supervisory authority, competent to supervise processing operations of the controller or a group of controllers within the Union.

To make the data subject's access to the supervisory authority easier, the GDPR regulates that the data subject may lodge a complaint with the supervisory authority first in the Member State of his/her habitual residence, place of work or place of the alleged infringement.

The supervisory authority is obliged to investigate the event which is the subject of the complaint, i.e. to ascertain whether the infringement in fact occurred and if so, to ensure rectification. The supervisory authority to which the complaint was lodged must also inform the complainant on the progress and the outcome of the complaint, including the possibility of a judicial remedy (please see below).

If the case requires further investigation or coordination with another supervisory authority, intermediate information should be given to the data subject. In order to facilitate the submission of complaints, each supervisory authority should take measures such as providing a complaint submission form which can also be completed electronically, without excluding other means of communication.

Right to an effective judicial remedy against the decision of a supervisory authority

Natural or legal persons

The GDPR grants each natural or legal person (i.e. also the controllers and processors) the right to an effective judicial remedy (i.e. to file a claim) against a legally binding decision of a supervisory authority concerning them. The purpose of this legal instrument is judicial review of a legally binding decision of a supervisory authority, if the person, to whom the decision relates, believes that the decision is incorrect.

The person affected by a binding decision of the supervisory authority can contest it by lodging a claim at the court. The decision may concern e.g. the exercise of investigative, corrective and authorisation powers by the supervisory authority or the dismissal or rejection of complaints. However, the right to an effective judicial remedy does not encompass measures taken by supervisory authorities which are not legally binding, such as opinions issued by or advice provided by the supervisory authority. Proceedings against a supervisory authority should be brought before the courts of the Member State where the supervisory authority is established.

Where the said court has a reason to believe that proceedings concerning the same processing[95] are brought before a competent court in another Member State, it contacts that court in order to confirm the information. If such proceedings are pending before a court in another Member State, any court other than the court first seized may stay its proceedings, apparently until the final decision of such proceedings[96]. Such court(s) may, on request of one of the parties, decline jurisdiction in favour of the court first seized if that court has jurisdiction over the proceedings in question and its law permits the consolidation of such related proceedings.[97]

Pursuant to Recital 143, any natural or legal person and also the affected supervisory authority which is the addressee of a Board's decision, has the right to bring an action for annulment of such decision of the Board before the EU Court of Justice.

Data subjects

Pursuant to the GDPR, each data subject has the right to an effective judicial remedy, i.e. a right to file a claim against the supervisory authority at a competent court, where the supervisory authority has not processed his/her complaint or did not inform the data subject within three months of the progress in processing the complaint or the outcome thereof. The purpose of this legal instrument is to grant the data subject the possibility of remedy against the inactivity of a competent supervisory authority.

Proceedings must be brought before the court of the Member State in which the supervisory authority is established.

Where proceedings are brought against a decision of a supervisory authority which was preceded by an opinion or a decision of the Board in the consistency mechanism, the supervisory authority forwards that opinion or decision to the court.

Right to an effective judicial remedy against the controller or the processor

Pursuant to the GDPR, the data subject has the right to file a claim at court where he/she considers that his/her rights under the GDPR have been infringed as a result of the processing of his/her personal data in non-compliance with the GDPR.

---

[95] E.g. proceedings with the same subject matter as regards processing by the same controller or processor, or the same cause of action.

[96] Refer to Article 11(2) of the GDPR; the principle preventing the possibility to maintain parallel proceedings in different Member States and the possibly to have them decided by contradictory decisions.

[97] Refer to Article 81(3) of the GDPR.

Proceedings against a controller or a processor are brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his/her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

Right to compensation and liability

The GDPR also grants each person (i.e. not just the data subject), who has suffered material or non-material damage as a result of an infringement of the GDPR, the right to receive compensation from the controller or processor for the damage suffered. The entity obliged to compensate such damage will be the controller or the processor, according to the circumstances of the case.

The controller's and the processor's liability for damage is regulated as follows:

- Each *controller* involved in processing is liable for the damage caused by processing which infringes the GDPR.
- The *processor* is liable for the damage caused by processing only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.
- Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are responsible for any damage caused by processing, each controller or processor will be held liable for the entire damage. That means that the data subject is entitled to claim the right to compensation of damage against any such entity. Where the controller or processor has paid full compensation for the damage suffered, that controller or processor is entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage.

The controller or processor will be exempt from liability if it proves that it is not in any way responsible for the event giving rise to the damage.

The court proceedings for exercising the right to receive compensation must be brought before the courts of the Member State where the controller or processor has an establishment. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his/her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers.

What now

Besides the obvious duty to comply with the obligations imposed by the GDPR on controllers and processors in connection with the processing of personal data, controllers and processors should carefully and in detail contractually agree their mutual rights and duties and the responsibilities arising thereof.

With regard to the joint liability for the entire damage against the damaged subject and with regard to the international character of legal relationships it is important to pay due attention to monitoring the legal existence and economic standing of the participating entities, legal proceedings initiated against them and to secure effective compensation of a proportional part of the compensation paid for damages by other controllers or processors.

Further information can be found here:

Recitals 141 - 147

Articles of Chapter VIII

Lesson 15 of 16

Sanctions and derogations

Below you will learn:

Important changes

- The GDPR substantially increases the maximum fines for the breach of obligations connected to personal data protection:
    - in cases of a more grave breach of the GDPR, the maximum amount of the fine is EUR 20,000,000 or, in the case of an undertaking, 4% of the of the total worldwide annual turnover of the preceding financial year (whichever is higher); the fine is up to CZK 10 million (Czech Rep.) and EUR 200,000 (Slovakia) so far;
    - in other instances, the maximum amount of the fine is EUR 10,000,000 or, in the case of an undertaking, 2% of the of the total worldwide annual turnover of the preceding financial year (whichever is higher); the fine is up to CZK 5 million (Czech Rep.) and EUR 50,000 (Slovakia) so far;
- The supervisory authority is not obliged to impose a fine for breach of the GDPR. However, if it is appropriate and purposeful with regard to the circumstances of the case, it may impose a difference measure (in addition to the fine or instead of it).

Compliance Action Plan

- Auditing the processing of personal data and accessing which processing operations are not compliant with the GDPR;
- Identifying areas with the highest risk and carrying out actions for mitigating the risk of fines;
- Considering the option to conclude insurance contracts for insuring the risks connected to personal data processing.

Sanctions

Administrative fines

When deciding whether to impose an administrative fine and its amount the supervisory bodies must give due regard to circumstances such as e.g. the nature, gravity and duration of the infringement (taking into account the nature, scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them), the intentional or negligent character of the infringement, any action taken by the controller or processor to mitigate the damage, the degree of cooperation with the supervisory authority, the categories of personal data affected by the infringement, etc.

If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of the GDPR, the total amount of the administrative fine must not exceed the amount specified for the gravest infringement.

In each individual case the imposition of administrative fines must be effective, proportionate and dissuasive.

The GDPR categorises various types of infringement into two main groups according to the graveness of the infringement, to which correspond different maximum amounts of the administrative fine:

Administrative fine of up to EUR 10,000,000 EUR or 2% of turnover

The first category includes infringements for which the GDPR allows the maximum administrative fine of EUR 10,000,000 or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. The respective obligations include:

- processing personal data relating to children in connection to information society services (Article 8);
- processing which does not require identification (Article 11);
- implementation of technical and organizational measures to ensure data protection by design and by default (Article 25);
- the obligation of joint controllers to agree their responsibilities for compliance with the obligations pursuant to the GDPR (Article 26);
- the obligation to designate a representative for controllers or processors not established in the EU (Article 27);
- obligations relating to the establishment of processors and obligations of processors (Article 28 a 29);
- the obligation to maintain written records (Article 30);
- the obligation to cooperate with supervisory authorities (Article 31);
- the obligation to ensure the safety of data and to report breaches (Articles 32 - 36);
- obligations connected to the appointment of a data protection officer (Articles 37 - 39);
- obligations of a certification body (Articles 42 and 43); and
- obligations of monitoring bodies (Article 41(4)).

Administrative fine of up to EUR 20,000,000 EUR or 4% of turnover

The second category includes infringements for which the GDPR allows imposing a fine of up to EUR 20,000,000 or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. These are infringements of the following obligations:

- obligations related to the principles for processing including consent (Articles 5 – 7 and 9);
- infringement of the data subject's rights (Articles 12 - 22);
- infringement of obligations related to the transfers of personal data to third countries or to an international organisation (Articles 44 - 49);
- any obligations pursuant to Member State law adopted under Chapter IX; and
- non-compliance with an order related to the flow of personal data by the supervisory authority and other related infringements (Article 58).

The Directive which is still effective delegates the Member States to adopt appropriate measures for ensuring its applicability, especially to introduce sanctions for breach of Member State laws adopted on its basis.[98]

The Czech legislative body has done so mainly in chapter VII "Administrative breaches", in articles 44 – 46 of the Czech Data Protection Act. A natural person in the position of a controller or a processor could be imposed a fine of up to CZK 1,000,000 for certain breaches, and up to CZK 5,000,000 if there are aggravating circumstances. Any natural person can be imposed a fine of CZK 1,000,000 for publishing personal data in contradiction to a restriction to do so regulated by a

[98] Article 24 of the Directive.

special Act[99]; for such breach conducted by means of print or radio media or via television or other similarly effective means corresponds to a fine of CZK 5,000,000. Legal persons may be imposed fines for such breaches in the amount of CZK 5,000,000 or 10,000,000.

The Slovak legislative body has done so mainly in chapter IV "Sanctions and publication of breach", in articles 47 – 71 of the Slovak Data Protection Act. Controllers and processors can currently be punished by a fine in the amount of EUR 300 – 200,000. A natural person who is not a controller or a processor, can be imposed a fine of EUR 150 – 2,000.

Other measures

Besides the power to impose an administrative fine pursuant to the above-mentioned principles, the supervisory authority also has the power to use other measures, i.e.:

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

Penal sanctions

In Article 84 and in Recital 149 the GDPR obliges Member States to determine rules for other, also criminal, sanctions for violating the GDPR,[100] including sanctions of seizure of profits acquired in connection with the breach. However, the principle restricting the imposition of two or more sanctions for the same act violating the GDPR should always be observed.

The Czech Criminal Code[101] already today regulates the crime of unlawful handling of personal data, which can be punished by imprisonment, monetary fine or punishment of restriction of

[99] Refer to Act no. 141/1961 Coll., on Criminal Procedure, as amended, and e.g. its provision about prohibition of publishing data about persons participating in a criminal procedure which do not directly relate to the criminal conduct; prohibition of publishing information on ordering or performance of telephone interception and records of telecommunication operations; restriction of announcement of information that violates the principle of presumption of innocence; prohibition of publishing information allowing identification of the identity of an aggrieved person of less than 18 years of age. Also see Act no. 218/2003 Coll., on the Administration of Justice in matters of minor persons, as amended, and a similar restriction on providing information on minors.

[100] Article 84 of the GDPR.

[101] Act no. 40/2009 Coll., the Criminal Code (Czech).

activities.[102] Pursuant to the Act on the criminal liability of legal persons and related proceedings[103], both natural and legal persons may face Criminal liability for the unlawful handling of personal data.

The Slovak Criminal Code[104] also regulates the crime of unlawful handling of personal data, which can be punished *inter alia* by imprisonment up to two years.[105]

Derogations and specific processing situations

The GDPR grants Member States the right to derogate from the wording of the GDPR, or (where the GDPR does not contain the respective provisions) to adopt their own legal regulation in the following affairs:

- national security, prevention and detection of crime;
- processing and freedom of expression and information;
- processing and public access to official documents;
- processing of the national identification number (birth number);
- processing in the context of employment;
- processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; and
- obligations of secrecy connected to professional confidentiality.

What now

We recommend controllers and processors carry out an audit to identify the most risky areas of processing operations and subsequently to prioritize steps for mitigating the risks of administrative fines or other sanctions. For this purpose it is suitable to access the extent of potential liability in connection with contracts with business partners, customers or suppliers, to which the controllers and processors are contractual parties, and to adjust the responsibilities between the parties accordingly.

To transfer the risk we recommend considering insuring the respective liability for loss caused by processing operations.

Further information can be found here:

Recitals 148 - 165

Articles 83 – 84 and Articles of Chapter IX

---

[102] See Article 180 of the Criminal Code: "(1) Who, even by negligence, unlawfully publishes, announces, makes accessible, otherwise processes or appropriates personal data, which was collected about another person in connection to the performance of public authority, and causes serious damage to the rights and legitimate interests of a person, to whom the personal data pertain, will be punished by imprisonment of up to three years or by prohibition of activities. (2)...".

[103] Act no. 418/2011 Coll., as amended.

[104] Act no. 300/2005 Coll., the Criminal Code (Slovak).

[105] Article 374 of the Criminal Code: "(1) Who unlawfully provides, makes accessible or publishes personal data about another person collected in connection to the performance of public authority or exercising of his/her constitutional rights, or personal data about another person collected in connection to exercise of work or employment or position, by which he/she breaches an obligation regulated by a generally binding legal regulation, will be punished by imprisonment up to one year. (2)..."

Lesson 16 of 16

Practical steps for ensuring compliance and minimizing the risk of sanctions

Summary of the School of Data Privacy

Over the past months we have provided you with detailed information about the new data protection legislation, which substantially alters the conditions regarding the lawfulness of processing. The GDPR *inter alia* extends the territorial reach of the European standard of data protection, whereby the new legislations's ambition is to ensure that the protection of personal data will apply to data subjects located in the Union, as well as if their data is processed outside the Union by subjects established elsewhere.

Further, the GDPR:

- obliges controllers to take a proactive approach to ensure the lawfulness of processing and to be able to demonstrate to supervisory authorities that they have carried out all necessary actions for ensuring compliance;
- regulates the principles which controllers should comply with when processing personal data, at the commencement of processing and at all times during the processing;
- changes the conditions for a data subject to provide valid consent with processing their personal data;
- substantially broadens the data subject's rights (e.g. the right to erase their data from the online environment or the right to personal data portability);
- regulates the controller's extensive information obligation towards data subjects and the obligation to actively communicate with data subjects in justified circumstances;
- increases the standard of security measures for the sake of personal data protection and obliges controllers and/or processors to report personal data breaches to supervisory authorities and/or data subjects;
- introduces new institutes by which controllers can ensure and demonstrate compliance, i.e. codes of conduct and certification mechanisms;
- regulates the obligation to keep records of processing activities, undertake a data protection impact assessment and consult the processing with a supervisory authority in advance;
- regulates the conditions of transfer of personal data to third countries and extends the possibilities to ensure the transfer is compliant;
- introduces a system of a single contact supervisory authorities for cross border processing the controller conducts within the Union;
- establishes substantially higher sanctions for violating the GDPR in comparison with previous legislation.

Timeline of practical steps for ensuring compliance

The GDPR will become effective in slightly less than 12 months, on 25 May 2018. With regard to the importance of the new changes, the extensive character of the matter and the amount of potential fines for noncompliance, we recommend controllers processing personal data (e.g. who employ persons) start carrying out the practical steps necessary to implement the GDPR's requirements without undue delay.

Below we present a list of necessary procedural steps as well as propose a feasible and realistic compliance timeline. We recommend keeping solid documentation of the process of the project of

compliance for the sake of being able to demonstrate due and professional care to the supervisory authority in the future.

- ✓ What: **Assigning a team of employees and securing financial and technical means for the project**

  When: July – August 2017

  How: First of all it is necessary to assign an employee / employees who will be responsible for (within the scope of their employment) ensuring the compliance of all the controller's processing operations with the GDPR. This also applies if the controller envisages assigning an external provider to develop and conduct the compliance project. In such case the responsible employee(s) will communicate on behalf of the controller with the external provider. Typically such employee can be a member of the legal or HR team, and for technical support the cooperation and awareness of an IT specialist is crucial.

  This project team will have to be provided with all required information and trainings so that they are well oriented in the matter and know what needs to be done.

  Multinational organizations or businesses must determine whether compliance with the GDPR will be handled on the local (national) level or if the local team will cooperate with headquarters.

- ✓ What: **Investigation of processing operations**

  When: August – October 2017

  How: The controller is obliged to determine (i) what personal data they process, (ii) what categories of data subjects are involved and (iii) what processing operations they carry out. This initial input must be determined with emphasis on the level of detail, accuracy, up-to-date state and completeness and the outcomes must be summarised in writing because they will be the starting point for further activities.

- ✓ What: **Analysis of discrepancies in light of the new legislation**

  When: October – December 2017

  How: The controller must conduct a thorough analysis of existing internal procedures of all concerned departments (e.g. HR, IT, departments having information about the software solutions at the controller, customer relations, receptionists identifying visitors, internal security, administrators of CCTV systems and other monitoring devices, etc.) – if they deal with personal data. Also, an analysis of documents regulating these internal procedures, if existing, is crucial.

  Based on the findings of the analysis a written report should be drafted, identifying shortcomings and risks and proposing suggestions for mitigating risks. The controller's top management should be acquainted with the report.

✓ What: **Data protection officials and processors**

When: October 2017 – December 2017

How: Controllers should verify if, as of the effective date of the GDPR, a data protection official must be appointed or not.

Contracts with processors and possible other persons should be reviewed to secure their wording complies with the GDPR. We recommend analysing the responsibility relationships of these persons regarding data protection, and the corresponding risks of compensation for damages and potential sanctions.

✓ What: **Developing or updating internal data protection policies**

When: January 2018 – March 2018

How: As of the effective date of the GDPR it is necessary for the controller to have implemented new or updated existing internal policies required by the GDPR. This will contain e.g. notifications of data subjects on processing personal data, document retention plans regulating the period of retention of certain documents containing personal data, consents with processing personal data, procedures to be followed in case of requests for data access, principles of protection of personal data, procedures to erase or block data, etc.

✓ What: **Implementing internal procedures**

When: March 2018 – May 2018

How: Controllers are obliged to implement internal procedures binding for employees handling personal data and to duly train them in respect to the tasks that will be required of them as of the GDPR's effective date. These procedures should regulate all general potentialities which can occur during the processing, e.g. in case of breach of the GDPR, data subject's requests for access to data, requests to erase or block data, etc.

Employees handling personal data must be demonstrably and in detail notified of their confidentiality obligation and of all implemented internal procedures regulating the processing, they must know how each relevant document template is used, how to communicate with data subjects, etc.

Of course, all required processing operations should be technically feasible, which should be ensured by an IT specialist.

✓ What: **Employee training**

When: February 2018 – May 2018

How: In order to raise awareness of the topic of data protection, controllers are obliged to provide trainings for employees handling personal data. The extent of risk and of potential sanctions for violation of the GDPR's provisions, which in certain cases can be as high as EUR 20,000,000 or 4% of the total worldwide annual turnover (whichever is higher), will directly depend on their qualification.

Where to start

The law firm Balcar, Polanský & Spol. s.r.o.'s team of professionals is ready to provide you with further information on any of the requirements mentioned above or any other aspects of the soon-to-be-effective GDPR. Therefore, please do not hesitate to contact our specialists below, or your usual contact person in our law firm.

You can learn more about our expertise, as demonstrated by our international certification in the data protection field, here:

http://www.balcarpolansky.cz/files/251/Focussed%20on%20DP_ENG.pdf

Contact person

For further information, please contact:

Slovakia:

JUDr. Helga Maďarová, CIPP/E, CIPM
Attorney | Certified Intl. Privacy Professional/Europe | Certified Intl. Privacy Manager

Tel.: +421 220 251 311
Cell: +421 917 092 076

helga.madarova@bapol.sk

Czech Republic:

JUDr. Jaroslav Srb
Attorney

Tel.: +420 220 251 111
Cell: +420 731 609 510

jaroslav.srb@bapol.cz