Assessment of the Draft Law on Personal Data Protection of Serbia

Desk study

Ljubljana, 28 May 2019

Matej Sironič

Anže Novak
The objective of the study is to assess the alignment of the new Serbian Personal Data Protection Act (hereinafter: the Law) with the EU acquis. The Law was adopted on 9/11/2018, which entered into force on 21/11/2018 and will enter into application on 21/08/2019. The Law was published in the Official Journal of the Republic of Serbia No 87/18 of 13/11/2018.

The assessment was done on the English translation of the Law (together with tables of concordance), provided by TAIEX via e-mail, dated 24/01/2019, which stated that the sent translation is based on the text of the Law adopted on 9/11/2018. Since this Assessment was done on the English translation possible misinterpretations may have occurred due to the possible inconsistency of the translation with the original text of the Law.

**GENERAL REMARKS:**

The intention of the Law is to harmonise the regulations with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation; hereinafter: GDPR) on one side and with the Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (also known as “Police Directive” or “Law Enforcement Directive”; hereinafter: LED).

**GDPR:**

The vast majority of the provisions of the Law follow GDPR and are in conformity with its provisions. Although the current law is insufficient with regards to sanctions and criteria for sanctioning. The Law is unclear regarding how the criteria form Art 87 for punishing the violations, will be observed in the misdemeanour procedure. Art 87 of the Law uses the word ‘administrative fines’ (same as GDPR), when in the penalties section the word ‘misdemeanour’ is used. Since we are not experts in Serbian penal legislation, we would only like to point out that there is no clear indication that the criteria from Art 87 will be used in determining the penalty according to the procedure that will apply in individual case. Furthermore, for several obligations, sanctions are lacking, which indicates the necessity for a thorough review of the penalties provision with reference to the Art 83 (4) to (6) GDPR.

A notion should be put to the fact that the Law itself does not further evolve principles, institutes and solutions, provided by the GDPR. In our opinion it is not in contradiction to GDPR also to regulate certain areas that are not included in the scope of GDPR with the national law, if such need arises. In this respect the protection of personal data of deceased individuals can be regulated. Furthermore, video surveillance, biometrics, records of entry to and exit from premises and other specific areas could be subject for specific regulation in order to avoid misinterpretation and legal uncertainty. For specific processing situations (archiving in the public interest, scientific or historical research purposes or statistical purposes, etc.) the Law could use an indicative approach to point to the specific national legislation that covers the named areas.

One of the main advantages of harmonisation with EU aquis could be that controllers and processors (especially micro, small and medium enterprises who would wish to make business cooperation with
partners or customers in Serbia and worldwide) could rely on the same standards for transfers as
applied in EU. It would be a significant practical value for such enterprises that they could for
example use standard contractual clauses adopted by the European Commission to create contracts
that would ensure them transfers from EU to Serbia and onwards. Same should than apply for other
mechanisms of transfers on the base of ‘appropriate safeguards’ where a specific authorisation from
the data protection authority is NOT required (especially: standard contractual clauses; binding
corporate rules; codes of conduct; certification mechanisms). The respective Law does not provide
for any “by default recognition” of appropriate safeguards approved according to GDPR by EU
competent authorities. Another suggestion for a solution could also be that the approved
appropriate safeguards according to GDPR could be valid in Serbia pending the affirmative decision
of a designated competent Serbian authority for each ‘appropriate safeguard’ (standard contractual
clauses, binding corporate rules, codes of conduct, certification mechanisms, etc.) already approved
by EU as such. The suggested solutions would contribute to a harmonic approach with transfers to
third countries using the same high standards for data protection as required by GDPR.

LED:

The provisions regulating processing by competent authorities for the purposes of the prevention,
investigation, detection or prosecution of criminal offences or the execution of criminal penalties,
including the prevention and protection of threats to public and national security; hereinafter:
special purposes of processing, are scattered all over the Law, making it difficult to read and
understand its aim and purpose.

The general approach of the Law, seen in many provisions, seems to be to stipulate in the final or
one of the paragraphs that the provisions of a certain Article or some of its paragraphs shall not
apply in case of data processing by competent authorities for the special purposes.

It would be more practical and comprehensive to use a different methodology, probably the best
solution would be to create a separate chapter of the Law. General provisions of the Law (chapters 2-
7 on principles, rights of the data subjects, controller and processor, transfer of personal data to third
countries or international organisations, the Commissioner, legal remedies, liability and sanctions)
could apply, and specific provisions governing exceptions from the general regime could be regulated
in this separate chapter. Exceptions should apply in particular to the purposes of processing, right of
access of the data subject, informing of the data subject, data quality, automated decision-making,
logging, transfer of personal data to third countries and other issues that need to be regulated
differently following the provisions of the LED. When listing the tasks and powers of the
Commissioner regarding processing by competent authorities for special purposes, it should be kept
in mind that this important issue should be regulated as far as possible in a similar way to the GDPR.
Powers of the Commissioner should be effective and enforceable. In that way both, LED and GDPR,
would be homogeneously interpreted and would in that way contribute to consistent and coherent
practice in the field of data protection.

This kind of methodology would make the Law more structured and most of all, easier to read and
more comprehensive.

The Law should also be clear and precise in determining that processing by competent authorities
which is performed for purposes other than for special purposes, falls under the scope of this Law
and is governed by its (general) provisions.

The Law contains several provisions aiming at (possible future) transposing of the LED into the
national legislation. Those provisions are in general in conformity with the LED, but unfortunately,
most of this provision only repeat the provisions of the LED, some of them are therefore very declarative, vague, bring no added value and do not contribute to legal clarity nor offer useful information that would facilitate the transposing of the LED and applicability of its provisions. On the contrary, they leave wide space for different interpretation and offer a wide discretion regarding their application. The sole definition of the "competent authority" is a good example – it only more or less follows the definition set in the LED. It does not further and more precisely determine the competent authorities in Serbia. This pose risks that in some cases authorities, bodies and entities on one side, as well as individuals (data subjects) on the other, will be in doubt regarding the nature of data processing and the rules that apply.

For certain obligations of the "competent authorities", sanctions are lacking, which also indicates the necessity of a more systematic approach to regulating the scope of data processing, the precise determination of authorities to which this special protection regime applies, as well as the amendment of other laws.

**LED and GDPR**

According to the practice of the European Court of Human Rights and European Court of justice, limitations to the fundamental rights and freedoms must be – as a general rule - prescribed by law. The limitation to the right of data protection is admissible only in so far as strictly necessary to achieve a legitimate purpose. The law must reflect legal clarity and certainty, so that individuals can predict with sufficient certainty when a legal provision will limit their right(s). The rights of the data subjects (access, rectification, restriction, to object, data portability, etc. according to GDPR and LED) form part of their right to data protection. Limitations to these derived rights have to meet same strict conditions in order for their limitation to be admissible. In particular LED places upon legislators an even greater burden to clearly and specifically prescribe the limitations to rights of individuals. In provisions such as in Articles 23 GDPR (restrictions) or 15.1 and 16.4 LED (limitation to the right of access), these provisions act as guidelines for national legislators to adopt specific and clear limitations to the rights of individuals. This requires specific legislative measures in specific areas where data subject rights necessarily need to be limited. A general data protection act may adopt similar or same provisions as the named GDPR and LED requirements, but they must not act as legal base for limitations themselves. They must point to the requirement of adopting specific legal provision that will observe the conditions set forth in the general data protection act. In other words, it must be left to the legislator to wage when a limitation of the right of the data subject is admissible, rather than rendering such power to controllers themselves (such as in provisions Art.28 Para I, Art. 34 Para II, Art. 40 of the Law). Such provisions open doors for arbitrary limitation of data subject's rights and this is not in conformity with European standards on the protection of personal data as a fundamental human right.

**OPINION ON INDIVIDUAL ARTICLES:**

**I. BASIC PROVISIONS**

**Art 1:**

Art 1, paragraph 2 uses the term 'in particular.' We suggest to replace it with the term 'also', since subject matter of LED is also part of the respective Law.

**Art 3:**
Article 3 of the Law does not contain any processing which would refer to the issue of the scope of its application in regards to Article 1, paragraph 2. We suggest the Law to be clear and precise in determining that all processing of personal data by competent authorities which is performed for purposes OTHER than for the special purposes (prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public and national security), falls under the general provisions of this Law – provisions that do not regulate processing performed for special purposes (ex. processing by the Police related to employment fall under the scope of general provisions). Such a solution would, in our opinion, significantly contribute to the legal clarity and certainty of the Law and the legal security of data subjects. If such solution is not provided, the data subjects could find themselves in an unclear position regarding the procedure of exercising their rights towards the competent authorities and possible limitations that may apply.

Art. 4:

The item 21 definition on ‘binding corporate rules’ (hereafter: BCR) rules is seemingly different from the definition in Art 4 (20) GDPR. Item 21 stipulates that BCRs refers to ‘internal policies’, although it is usually an agreement signed between legally separate entities, so that it is not inherently ‘internal’ (even though these entities usually operate as a controlling and its controlled entities).

With reference to Art 4 (20) GDPR – the definition of entities who can adopt BCRs is also different. GDPR stipulates that BCRs can represent a legal base for transfers to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity; Item 21 of the respective Law stipulates that BCRs can be adopted: for the purpose of regulating the transfers of personal data to a controller or processor in one or more countries within the multinational company or group of undertakings. Considering the definition of ‘multinational company’ in Item 19 of the respective Law, the scope of entities who can adopt BCRs approaches the GDPR definition, although, different wordings and criteria can exclude certain economic activities or business for which the possibility to adopt BCRs according to GDPR would exist. In conclusion it would be advisable to align wording of definitions in the respective Law to GDPR, since one of the primary goals of harmonisation is also to harmonise criteria for transfers, so that companies that transfer data from EU to Serbia and onwards can rely on the same standards. Any distinction in the terminology and criteria used can result in a situation that approved BCRs by lead supervisory authority form EU (that allow for example transfers from EU to Serbia and onwards to India) might not be approved by the Commissioner of the Republic of Serbia. In this way businesses from EU may not be encouraged to transfer data to Serbia due to administrative barriers (or even only for the fear from possible administrative barriers).

II. PRINCIPLES

Art 7:

Recital 26 of the LED stipulates that Member States should lay down appropriate safeguards for personal data stored for longer periods for archiving in the public interest, scientific, statistical or historical use. Art 7, paragraph 3 of the Law stipulates that processing by the same or another controller may include archiving in the public interest, scientific, statistical or historical use, for the purposes set out in Article 1(1), subject to appropriate safeguards for the rights and freedoms of data subjects. The Law does not supply the appropriate safeguards as required by R26 LED in an adequate and sufficient manner (Art 92 of the Law is also insufficient with regards to the appropriate safeguards as referred to by R 26 LED).
Art 8:

LED (Art 5) leaves it open to national legislators to provide for either appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. In any case, procedural measures should ensure that those time limits are observed. Deriving from the Law it only stipulates that, if the time limit is not determined by law, the controller shall determine the time limit. The law does not determine the deadlines neither establishes the criteria the controller should use and follow when determining the time limits.

National law should set maximum storage periods as well as provide clear, objective and precise criteria on which the decision to keep data for a longer period of time should be based. Supposing that national laws, regulating competent authorities and their data storage, do not impose the obligation to perform periodic reviews of the need for storage of specific type of data, the general data protection law should set an example and provide this obligation and the appropriate criteria. The decision to further keep the data and the criteria used to accept this decision should be transparent and made available to data subjects and the Commissioner.

Under paragraph 4 the Commissioner “monitors the compliance with the time limits in line with its competences prescribed by this Law.” The Law does not contain any penalty provision for this matter and therefore it is not possible to identify the liability in the event of a breach.

Art 9:

We wonder what is the reason for a distinction between item 1) and 2) in the Law. LED (Art 6) does not differentiate between different levels of suspicion (see Art 6(a) LED) which of course does not prevent the national law from making such a distinction, although this distinction should be well-grounded and bring added value. We cannot recognise the added value in this solution.

Art 10:

It is not clear in what way/how the personal data based on facts will be distinguished from those based on personal assessments. Will these data be, for instance, marked or equipped with a specific symbol or letter or similar solution? Personal assessment should be subject of periodical review. We recommend to establish how often does this review take place (after a certain time period or subject to change of relevant circumstances).

Art 11:

In comparison to LED, the Law stipulates (paragraph 3) that the competent authority transferring personal data shall provide, to the extent possible, necessary information enabling the assessment of the degree of, not only accuracy, completeness and reliability, but also verifiability of the data. Verification procedure enables the competent authority to assess accuracy, completeness and reliability of the transferred data and this information should be provided to the recipient. Accuracy, completeness and reliability refer to data quality, while verifiability refers to the procedure of acknowledging facts and other circumstances, enabling assessment of the data quality. The recipient will assess accuracy, completeness and reliability of the data and not their verifiability.

In paragraph 4 the Law does not predict possibilities/situations when it emerges that data transmitted were incorrect or unlawfully transmitted. This might be identified by the controller, the recipient, the user, the Commissioner or other person involved.

Also, the Law regulates this situation (incorrect data transmitted or unlawful transmission) only when the data is transmitted to competent authority. It does not regulate transmitting to other possible
recipients. In any case, all of the recipients should be notified of that kind of transmission, not only the competent authority. Therefore, we advise that the Law is amended in that way.

Art 15:

Paragraph 4 stipulates that when assessing whether consent is freely given, “utmost account shall be taken of whether the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.” Utmost account of these criteria should definitely be taken and this is the most important, but yet not only criteria that should or might be taken into account. The current formulation might mislead controllers or processors, when assessing consent that this is the only criteria that has to be taken into account. Therefore, the solution in GDPR Art 7, paragraph 4 (“inter alia”), would be more suitable.

Art 16:

Paragraph 2 is a bit unclear when it stipulates that consent shall be given “by a parent exercising parental rights” or legally authorized holders of parental responsibility. Does this especially cover situations when one of the parents has lost his parental rights? If not, does it mean, in case of both parents jointly exercising the parental rights, that consent of one of them is enough or the consent of both is mandatory? It should be considered from the perspective of national legislation which regulates parental responsibility, if the wording and formulation of this article is coherent to that legislation and if it sufficiently responds the question on who should in individual case provide the consent (one or both parents).

Art 17:

In paragraph 2, item 3), we suggest to delete “due to the lack of legal capacity”. The processing of special categories of personal data shall be allowed in accordance with this item (3) if the data subject is physically or legally incapable of giving consent. Both options of incapability (physical and legal) are included. The data subject could be legally capable of giving consent but physically unable to do so. **THERE MAY BE INCONSISTENCY IN TRANSLATION WITH REGARDS TO THIS COMMENT.**

Art 18:

Item 3) stipulates that processing of special categories of personal data shall be allowed when processing refers to specific categories of data which are manifestly made public by the data subject. The Art by itself regulates processing of special categories of personal data. Therefore, it is questionable why does item 3) contain the term “specific categories of data”? If it refers to special categories, this addition is not necessary. If it refers to specific categories within special categories of personal data, then it should further evolve the provision and clearly explain its meaning.

It has to be taken into account that processing of specific categories of personal data requires even more precise and solid justification than processing of other personal data and the provisions governing it should be clear and leave no room for discretion or different interpretation. That includes also clarity for the data subject who makes his data public. He must be, at the time when doing this, aware of the fact that the data will be publicly available to everyone, including competent authorities. **THERE MAY BE INCONSISTENCY IN TRANSLATION WITH REGARDS TO THIS COMMENT.**

Art 19:

Paragraph 1 refers to personal data relating to inter alia ‘security measures’. It is not clear from this provision if personal data from ‘security measures’ refer only to security measures regarding criminal convictions and offences or to security measures for data processing in general. The purpose of EU
aquis is that special regime referred in this Article only applies for personal data relating to criminal convictions or criminal offences.

III. RIGHTS OF THE DATA SUBJECT

Art 21:

Paragraph 9 of the Law does not provide for any reference to the procedural requirements or practice with regards to standardised icons following the requirements from Art 12 (8) GDPR. Such a reference to the EU procedural requirements or practice could contribute to a harmonic approach on this area, which would ease the free flow of data.

For Paragraph 10, please observe general remarks regarding the methodology for harmonisation with LED.

There is no sanction for the violation of this article. According to GDPR, for the violation of Art 12 GDPR, the penalty is up to 20.000 or 4% of worldwide turnover (whichever is considered a greater violation).

Art 22:

See the commentary to Art 29 regarding the right to rectification according to Article 16 (1) LED.

There is the sanction for the violation of this article and it should be provided for.

Art 25:

The wording 'the law may prescribe' in Paragraph 4 is not in accordance with the GDPR requirements (appropriate would be 'the law shall prescribe'). Any limitation to the rights of individuals (including the transparency of processing) has to be prescribed by law. The provision from 13 (3) LED stipulates: "Member States may adopt legislative measures delaying, restricting or omitting the provision of the information to the data subject...". The word may in this sentence refers to the possibility of adopting legislative measures that correspond to certain conditions laid down by 13 (3) LED. If such measures are not prescribed by law, then the limitation to the right to inform data subjects would not be admissible (see general remarks).

Art 28:

The title does not reflect the content of this article, which refers to the right to access of data processed by 'competent authorities for special purposes'.

In Paragraph 1, Item 2), suitable substitute for the word 'enable' would be to 'avoid prejudicing' as in 15(1)(b) LED.

The limitations must be prescribed by law (see general remarks).

Art 29:

Right to rectification that is regulated under this article seems to cover both, Right to rectification from Art 16 GDPR and the right from 16 (1) LED (since the Law does not contain any provision that Art 29 the Law would not apply for the 'processing by competent authorities for special purposes'). According to procedural provisions from Art 22 – that regulates costs, accessibility, etc. for the rights of individuals when competent authorities are processing personal data for special purposes – Right to rectification from Art 29 is not included in Art 22. Since Art 22 does not apply for Art 29, this Law does not adequately guarantee the right to rectification from Art 16 (1) LED to the data subjects.
Art 30:

Paragraph 4 stipulates that data subject shall submit the request for erasure to the controller. Such provision is not included in GDPR Art 17. It is not clear why such provision is required. This provision should not affect the obligation of the processor to assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller’s obligation to respond to requests for exercising the data subject’s rights (when for example data subject would file his request to exercise his rights with the processor). If the processor could lawfully refuse to act upon receiving a request for erasure, by stating that data subject should according to para 4 Art 30 of the Law submit the request for erasure to the controller – in this case, such exception would be in contradiction to the purpose set by the GDPR.

Art 32:

Paragraph 1 item 2) stipulates that personal data will be maintained and restricted processing despite that data subject has filed a request for erasure in case when the data have to be collected and maintained for the purpose of evidence. This provision is not completely in line with a corresponding provision from 16.3 (h) LED. It is also not logical that the controller needs to maintain data that yet need to be collected (data that still have to be collected are not yet in the possession of the controller, therefore data subject cannot request for erasure of such “possible future” data nor can the controller restrict processing of such data).

Art 34:

The limitation to the right to access as set forth in Para 2 of Art 34 should be regulated by a special law (lex specialis). The provisions from Paragraph 2 should only be regarded as general guidance for the legislator. This remark concerns the alignment with the EU aquis. The provision that would in line with GDPR could be, for example: “The specific law may prescribe that the controller shall be wholly or partially released from the obligation to inform, referred to in Para 1 of this Article, to the extent to which that release of obligation constitutes a necessary and proportionate measure in a democratic society, with due regard for the fundamental rights and legitimate interests of the natural person concerned, in order to...” (see the last paragraph in general remarks).

Art 35:

In accordance with Article 17(1) LED, national legislation has to foresee the possibility to exercise the rights to information, access, or information about refusal of rectification or erasure by the controller through the competent supervisory authority when these rights have been restricted by the controller on the basis of legislative measures allowing for restrictions, and not where these rights could be exercised directly with the controller (indirect access). Paragraph 1 of Art 35 of the Law, stipulates that the rights in the aforementioned situations can be exercised through the Commissioner and on the basis of its competencies prescribed by this law. The Law in the competencies section does not specifically regulate that the Commissioner will handle individual requests within the meaning of indirect access. From the wording in paragraph 1 derives that the Commissioner will act only on the basis of its competencies prescribed BY THIS Law, while this Law does not contain any specific competence regarding indirect access. Therefore, it is questionable, if the indirect access from 17(1) LED is afforded by this Law. In conclusion, the respective Law is not sufficiently clear and precise regarding the indirect access from 17(1) LED.

Paragraph 3 stipulates that the Commissioner shall inform the data subject inter alia of the right to address the court for the protection of his or her rights. In comparison to 17 (3) LED that uses the
worrying 'of his or her right to seek a judicial remedy', the respective Law is less clear that individual should be informed about a specific judicial remedy to the administrative court regarding the procedure before the Commissioner (not that the individual has the possibility to address any court regarding his right to data protection in general). The WP29 opinion on this matter clearly indicates that precise information should be given to a data subject as to which judicial authority is competent, either by providing its contact details and/or the reference of the relevant legal provision in order to facilitate the data subjects' enquiries. Paragraph 3 does not clearly indicate that individual should be provided with information on judicial remedy regarding his or her right through indirect access.

Art 38:

Paragraph 1 stipulates that the data subject shall have the right that the decision made solely on the basis of automated processing, including profiling, is not applied to him or her, if such decision may produce legal effects concerning the data subject or significantly affect his or her legal position. The Article 22 (1) GDPR stipulates that the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. GDPR prohibits that automated decision-making has an effect on individual in two situations. The first refers to 'a legal effect', which means to affect someone's legal rights, such as the freedom to associate with others, vote in an election, or take legal action. A legal effect may also be something that affects a person's legal status or their rights under a contract. Examples of this type of effect include automated decisions about an individual that result in: cancellation of a contract; entitlement to or denial ofa particular social benefit granted by law, such as child or housing benefit; refused admission to a country or denial of citizenship. The second, 'similarly significant affect,' refers to a decision-making process that does not have an effect on people's legal rights, though it could still fall within the scope of Article 22 GDPR if it produces an effect that is equivalent or similarly significant in its impact. In other words, even where there is no change in the person's legal rights or obligations, the data subject could still be impacted sufficiently to require the protections under this provision. The GDPR introduces the word 'similarly' (not present in Article 15 of Directive 95/46/EC) to the phrase 'significantly affects'. Therefore, the threshold for significance must be similar to that of a decision producing a legal effect. Recital 71 GDPR provides the following typical examples: 'automatic refusal of an online credit application' or 'e-recruiting practices without any human intervention'. For data processing to significantly affect someone the effects of the processing must be sufficiently great or important to be worthy of attention. In other words, the decision must have the potential to: significantly affect the circumstances, behaviour or choices of the individuals concerned; have a prolonged or permanent impact on the data subject; or at its most extreme, lead to the exclusion or discrimination of individuals.

Wording in paragraph 1 does not clearly reflect the two explained concepts from Article 22(1) GDPR, namely 'legal effects' and 'similarly significant effects'. Wordings in paragraph 1 -- decisions that 'may produce legal effects' -- is too vague as to the concept of 'legal effects' from GDPR and at the same time does not cover 'similarly significant effects'. The wordings from paragraph 1 as to the decisions that 'significantly affect his or her legal position' again do not fit completely to any of the two mentioned concepts from GDPR. In conclusion, the suggestion would be to adjust the wording to the

---

2 WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, Revised and Adopted on 6 February 2018, p.21, 22.
one used by GDPR in Article 22(1). THERE MAY BE INCONSISTENCY IN TRANSLATION WITH REGARDS TO THIS COMMENT.

Art 40:

Paragraph 1 stipulates:

The rights and obligations provided for /.../, may be restricted in so far as these restrictions respect the essence of the fundamental rights and freedoms and if it is a necessary and proportionate measure in a democratic society for:

The Article is inconsistent with GDPR and LED that only a specific legislative measure may restrict data subject’s rights. Article 40 (with reference to Art 23 GDPR) should be regarded as a general framework for the legislator to regulate specific areas where data subject rights necessarily need to be restricted, rather than guidelines for controllers to decide when it would be suitable to restrict data subjects’ rights. According to the EU aquis deriving from judicial practice of ECI and recognised standards from ECHR, only specific and clear legal provision may restrict fundamental rights of the data subjects (see last paragraph of the general remarks). A provision that would adequately observe GDPR requirements could for example stipulate:

The rights and obligations provided for /.../, may be restricted by a special legislative act in so far as these restrictions respect the essence of the fundamental rights and freedoms and if it is a necessary and proportionate measure in a democratic society for:

Art 23 (2) GDPR is intended to guide national legislators to adopt specific legislative provisions that are sufficiently precise, so that they ensure legal clarity and certainty when limiting the scope of fundamental rights and freedoms of the data subjects.

Considering all of the above mentioned, Article 40 is not in line with the EU aquis (see also general remarks).

Paragraph 3 stipulates that same applies also for processing by competent authorities which is not performed for special purposes. It should be duly noted that all processing of personal data by ‘competent authorities’ that are not performed for ‘special purposes’ should fall under general data protection regime (see general remarks).

IV. CONTROLLER AND PROCESSOR

Art 41:

GDPR imposes on the controller an obligation to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR. The Law stipulates that controller shall implement appropriate technical, staffing and organisational measures. Staffing measures are related to personnel and are as such part of organisational measures. Therefore, there is no need to specifically name them in the Art. It also offers the possibility of misinterpretation that staffing (personnel) measures are of higher importance than other organisational measures. Therefore, we suggest the omission of the word “staffing”. This goes also for other Articles of the law stipulating the same text.

Art 42:

We suggest that the title of the Art follows GDPR: “Data protection by design and default”. It is a vital and important principle (data minimisation) of the GDPR which clearly divides the time of the
determination of the means for processing and the processing itself while having in mind each specific purpose of the processing and should thus be followed to ensure that requirements of the GDPR are met.

According to paragraph 3, measures referred to in paragraph 2 shall ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of natural persons. The current formulation might mislead the controllers that this is the only objective that measures referred to in paragraph 2 shall ensure. Therefore, the solution in GDPR Art 25, paragraph 2 ("in particular"), would be more suitable.

Art 44:

Paragraph 3 stipulates that complaint, lawsuit or other legal actions referred to in this Law, could be lodged against the controller or the processor. We wonder if the national legislation of the Republic of Serbia maybe provides other legal actions that could be lodged against them in accordance with other national law? If this is the fact, then the provision should be considered for amendment in that sense.

Art 45:

Paragraph 4 determines the content (8 obligatory categories) of the contract or other legally binding act between the controller and the processor. These categories are not exhaustive according to GDPR and other contents may be included. Therefore, the solution in GDPR Art 28, paragraph 3 ("in particular"), would be more suitable.

Paragraph 5 stipulates that the processor shall inform the controller, without undue delay, if it deems that the written instruction received from the controller is not in line with this Law or other law governing personal data protection. The time period ("without undue delay") is a bit vague, especially in comparison to the one set in the GDPR ("immediately").

Paragraph 7 stipulates in the last sentence that if another processor fails to meet its obligations in relation to personal data processing, the processor shall remain fully liable for the performance of these obligations of another processor. According to GDPR, the processor remains fully liable to the controller. Does this provision of Law refer to liability also to other subjects (data subjects)?

Art 47:

Paragraph 3, item 6) uses the term “types” of transfers. The commonly used term is “categories” of transfers.

Paragraph 7 stipulates that the records shall be kept permanently. Nor GDPR nor LED determines permanent keeping of the records. The principle of storage limitation should be taken into account. The controller or processor may at some point due to changed circumstances no longer be obliged to maintain such record and the need to keep the records permanently should be an exception (a very well-grounded one) and in no case a general rule.

It should also be clearly stipulated that the last paragraph does not apply to competent authorities when processing personal data for special purposes in accordance with LED.

Art 48:

Penal provision (Art 95, paragraph 2, item 5) on this Art is not complete, since it only covers not recording processing actions. The controller or processor might record them but not in a sufficient way to determine the facts, provided in paragraph 2 or are those logs used for purposes, not foreseen in this Article.

The national legislation should further establish requirements for logs, especially their content, adequate storage periods and technical measures to guarantee their integrity. Logs should be an important issue when designing the data protection by design requirements (Art 42 of the Law).
Art 50:

Paragraph 2 begins with words “Where it is necessary ...”. This sentence may cause misinterpretation. The circumstances that have to be taken under consideration are stipulated in paragraph 1 and there is no need for additional test of their necessity in paragraph 2.

In paragraph 5, we believe it is important to emphasize that ALL natural persons who act under the authority of the controller shall act only on the basis of his instructions. Therefore we suggest adding the word “any” before the word “natural”.

Art 52:

Art 30 (6) LED deals with the situation where the breach of personal data processed by competent authorities for special purposes involves personal data that have been transmitted BY OR TO the controller of another Member state. The situation to transmit data BY the controller is not covered by paragraph 8, article 52 of the Law. This situation could also be prescribed pending international agreement that would impose such an obligation to a third country or international organisation.

Art 53:

In the last paragraph we suggest to add the possibility that the controller may also omit communication to the data subject, not just delay or restrict it.

Art 54:

From paragraph 6, item 4) derives that the description of measures that will address the risks regarding DPIA, include legal safeguards, security measures and technical, organizational and staffing measures. Those measures are, as also stipulated by Art 50 of the Law, part of the security measures. The purpose of a corresponding provision from GDPR (35(7)(d) GDPR), which uses the word “measures” is to address all possible risks regarding data protection with individual processing activity (e.g. lawfulness – what is the appropriate legal base and how will it be assured; transparency of processing – how to adequately inform data subject about individual processing activity; data subject rights – how will the controller deal with requests of data subject, etc.). All aspects of personal data protection should be observed, not only the security aspects. Therefore we suggest amending this article so that DPIAs will not only describe security conditions, but encompass a total review of all important aspects of data protection (lawfulness, transparency, data minimisation, etc. – with regards to the recognised risk).

Art 55:

The deadlines set in this Article should follow the deadlines set in the GDPR.

We believe that Paragraph 7, item 3) is not clear to establish that measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Law should be communicated to the Commissioner – not only the security measures (see comment to Art 54 of this law). We suggest amending the Law in this respect.

Art 56:

The final paragraph stipulates that the Commissioner shall prescribe the form of the record of data protection officers and shall regulate the manner of its keeping. This should be added to the tasks of the Commissioner, regulated by Art 78 of the Law.

We recommend that the Law also prescribes more specific conditions for designation data of protection officer for public authorities or bodies, with regards to his education, expertise, skills and experience in the field of personal data protection.

Art 57:
The independence of data protection officer that the controller and processor shall ensure according to paragraph 3, is not specified within the current text of the Law. What kind of independence (financial, organisational, professional, ...) shall be ensured?

Art 59:

In our opinion Para 1 Item 11) is not clear enough to stipulate that codes of conduct should concern methods of peaceful dispute resolution for resolving disputes between controllers and data subjects with regard to data processing. This should be clear in order to avoid any misinterpretation about the nature of disputes.

Regarding Para 2 we advise to make reference to the territorial scope of the law to clearly describe, which controllers or processors are not subject to this Law. For instance: "...the controllers or processors that are not subject to this Law, pursuant to Art 3 Para 3 or Para 4 may also commit or adhere..."

Furthermore regarding Para 2, it should be clear that the safeguards provide the rights to the data subjects. For instance: "... via contractual or other legally binding instruments, to guarantee implementation of all appropriate safeguards, and in particular in relation to the rights of the data subjects."

Paragraph 3 should clearly stipulate that a code of conduct shall contain mechanisms (not provisions) that enable the monitoring of compliance. It should also be clearly stipulated that this monitoring is mandatory and, since it refers to the provisions of Art 77 to 79, that mechanisms are without prejudice to the tasks and powers of the Commissioner, not only (control and other) powers as stipulated in the Law.

Art 60:

According to Para 1 an entrepreneur or other legal body pursuant to the law governing accreditation may be accredited for monitoring the adhered codes of conduct. According to paragraph 3 Item 1) and 4) the Commissioner is, by giving his opinion, also taking part in this procedure. The relation between the law governing accreditation and the Law is unclear. We suppose that the law governing accreditation does not specifically prescribe role of the Commissioner, nor as a body which issues accreditation nor as a participant of any kind in the procedure. Art 78 of the Law which lists the tasks of the Commissioner, also does not provide for any task of such kind.

The competences of individual authorities should be clarified by law – we would advise, that the Law makes clear which authority is competent for issuing the accreditation and what, if any, is the role of the Commissioner in the process. This would avoid a possible competence dispute and other issues regarding the procedure.

Art 61:

Paragraph 1 stipulates that data protection certification mechanisms and data protection seals and marks may be established taking into account the specific needs of small and medium-sized enterprises. We cannot see the reason to leave out micro-sized enterprises.

Art 62:

Paragraph 1 stipulates that the certification body is accredited pursuant to the law governing accreditation.

Paragraph 2 includes the Commissioner (his opinion) into the certification procedure, while paragraph 3 clearly stipulates that the Commissioner shall determine the criteria for accreditation of certification bodies pursuant to conditions referred to in Paragraph 2. It is also clearly stipulated that the certification body can be accredited only if it provides proof to the Commissioner that it meets the conditions prescribed by paragraph 2.
The Art 78 of the Law which lists the tasks of the Commissioner, does stipulate that the Commissioner prescribes and publishes the criteria for accreditation of a certification body pursuant to Article 62 of this Law. It does not mention giving opinions in the process.

The competences of individual authorities should be clarified and the Art should be considered for amendment in that way. The role of the Commissioner in the process has to be clearly prescribed. This would avoid a possible competence dispute and other issues regarding the procedure. V. TRANSFER OF PERSONAL DATA TO THIRD COUNTRIES OR INTERNATIONAL ORGANISATIONS

Art 64:

Term 'appropriate level of safeguards' from the title may raise confusion due to the fact that Art 65 of the Law uses the term 'appropriate safeguards'. A more suitable term, though the same as in GDPR, would be 'adequate level of protection'. On different occasions in Art 64 also the term 'adequate level of protection' is used. We suggest a more coherent approach in using terminology, since the terms 'appropriate safeguards' and 'adequate level of protection' bare a different meaning.

According to Art. 45(3) GDPR the Commission must adopt an implementing act to enforce an assessment that a third country or international organisation affords an adequate level of protection (adequacy decision). Such an implementing act also has to prescribe the mechanism for a periodic review, at least every four years, which shall take into account all relevant developments in the third country or international organisation. The requirement from Art 45(3) GDPR (for a mechanism for a periodic review that has to be prescribed by an implementing act) is not adequately observed within the solution of the Law. Paragraph 4 Art 64 of the Law regulates the possibility of the Republic of Serbia to adopt international agreements according to which the transfers to third countries would be allowed. Paragraph 5 Art 64 stipulates that in the process of ratification of an international agreement on personal data transfer, the fulfilment of the conditions referred to in Para 3 of this Article shall be specially determined. The named conditions from Para 3 refer only to the conditions for a recognition that a third country or international organisation affords adequate level of protection. It does not on the other hand require for a mechanism for a periodic review from Para 6 Art 64 to be prescribed or agreed with an international agreement (the government shall continuously monitor developments with regard to personal data protection in a third country, parts of its territory, areas of activity, or in an international organisation, on the basis of information collected directly and taking into account information collected by international organisations, which are important for reviewing the existence of an adequate level of protection). A requirement for a linking factor to this particular requirement from Para 6 is not required by this Law. In our opinion this is important for the alignment with EU aquis. International agreements that will Serbia make to other countries are legally binding commitments which will affect data subjects, therefore any accepted international agreement by the Serbia should take into account the mechanism for a periodic review in order to fully align with EU aquis on this matter.

Art 65:

According to paragraph 1, the transfers are possible to countries that are not on the list from Art 64 paragraph 7. Art 64 Para 7 includes two lists, including the list of countries that do not assure adequate level of protection (anymore). The provision from Para 1 Art 65 has no clear indication as to what list it refers to. It would be in contradiction to the purpose of this provision if the prohibition from Art 65 Para 1 would apply for the list of countries that do not assure adequate level of protection — therefore transfers to those countries would not be possible (not only on the basis of adequate level of protection, but according to Para 1 Art 65 it would also not be possible to transfer data on the base of appropriate safeguards). Such an interpretation would be in contradiction to the
purpose of a similar provision in GDPR (Art 46(1)), which is intended that controllers should not seek for appropriate safeguards when they are transferring personal data to a country which already affords adequate level of protection. In conclusion, Art 65 Para 1 of the Law does not clearly indicate to the list of countries that DO provide adequate level of protection – which may cause confusion and misinterpretation in practice.

Paragraph 2, item 2) stipulates that standard contractual clauses (SCC) can be a legal base for transfers. The possibility to use SCCs according to GDPR facilitates transfers. In the boundaries of present solution, it can easily occur that transfers from EU to Serbia and further transfers to third countries that depend only on the SCC adopted by the EU Commission, will be in violation of this Law. In result, EU based multinational companies will be less encouraged to make business in Serbia due to additional administrative obstacles with data transfers, which is not the goal of GDPR. A consideration should put regarding possible amendment of this Article.

Paragraph 2, item 2) also stipulates that SCC can only be the legal base for processing between a controller in Serbia and a processor in a third country. There are two models of SCC adopted by the EU Commission currently available – first, for transfers between controller and processor⁴ and second, between controller and another controller⁴. In the case of controller –controller transfer, the mechanism presented in the Law, fails to assure lawful transfers based on such SCCs. Also processor-processor transfers are possible in practice, but according the currently available SCCs adopted by the Commission do not render that possibility yet. A consideration should put regarding possible amendment of this Article.

The conditions for the appropriate safeguards should closely follow GDPR. The respective Law in current text astrey from the wording and concepts in GDPR, especially regarding SCCs and BCRs (see also comment to Art 4). In our opinion a higher level of harmonisation could be achieved. One of the main advantages that GDPR introduces with transfers on the base of “appropriate safeguards” for controllers and processors (especially micro, small and medium enterprises who would wish to make business cooperation with partners or customers in Serbia and worldwide) – is that they can make transfers without additional approval by national supervisory authority - solely by using mechanisms from “appropriate safeguards” (especially: standard contractual clauses; binding corporate rules; codes of conduct; certification mechanisms). The main advantage of alignment with the EU aquis would be that those companies could rely on the same standards for transfers as adopted in EU also elsewhere. It would be a significant practical value for such enterprises that they could for example use standard contractual clauses adopted by the European Commission to create contracts that would ensure them lawful transfers from EU to Serbia and onwards (and not worrying that EU SCCs would not be valid according to Serbian standards). Same should than apply for other mechanisms of transfers on the base of ‘appropriate safeguards’ where a specific authorisation from the data protection authority is NOT required. The respective Law does not provide for any “by default recognition” of appropriate safeguards approved according to GDPR by EU competent authorities. Another suggestion for a solution could also be that the approved appropriate safeguards according to GDPR could be valid in Serbia pending the affirmative decision of a

⁴ Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC.
COMMISSION DECISION of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries.
designated competent Serbian authority for each ‘appropriate safeguard’ already recognised by EU as such.

Art 66:

In Paragraph 1, a clear reference to the list of countries that assure adequate level of protection is not provided for (see also comments to Art 65 Para1).

VI. THE COMMISSIONER

Art 74:

Even though GDPR does not require for specific education, expertise, experience, etc. for supervisors, it would in our opinion be valuable if such requirements existed. Since we are not experts in Serbian legislation, we can assume that these issues are regulated by another law – although deriving from paragraph 4 (The Commissioner independently carries out the selection of employees among candidates who meet the conditions for work in state bodies prescribed by law, and manages them completely autonomously) it is not clear that such requirements are in fact prescribed.

Art 77:

The supervisory authority is competent for the performance of the assigned tasks and the exercise of the powers, not only exercise of the powers as derives from this Article. We suggest to consider amending this Article in this respect.

Art 78:

When listing tasks, the Law does not list the task of checking the lawfulness of processing (verification) pursuant to Art 35 of processing and informing the data subject.

Monitoring according to item 9) should in particular, but not exclusively, comprise relevant developments of information and communication technologies and commercial practices, relevant for the protection of personal data.

Item 22) stipulates that the Commissioner shall fulfil any other tasks in accordance with this Law. Having in mind that the Law contains some references to other national legislation, it is important to check whether these laws maybe stipulate any other task of the Commissioner in the field of the personal data protection.

In paragraph 7 we suggest to replace the word “complaints” with the word “requests” since it covers all types of filed applications and the word “or” with the words “in particular”. The requests may be excessive in particular because of their repetitive character so this is the clarification of excessiveness.

Art 79:

The first item of the paragraph 3 should be amended, in accordance with the abovementioned comments on Art 65. The transfers are also possible between controller and controller. For such processing there is no legal ground to adopt SCC in the current version of the Law. It would also be possible to transfer data between processor and another processor. Even though this type of SCC is not currently available they can be adopted by the Commission.

We suggest the last paragraph to stipulate that the Commissioner, in case of infringements of the Law, may initiate or engage otherwise in a procedure before the court or other (judicial) authority in order to enforce the provisions of this Law.

VII. LEGAL REMEDIES AND SANCTIONS
Art 85:

Art 85 stipulates that data subject has the right to mandate a representative of the association engaged in protection of rights and freedoms of data subjects, and in connection to the protection of personal data, to represent him in legal proceedings regarding data protection. According to Art 80 (1) GDPR such association has to be properly constituted in accordance with the law of a Member State, has to follow statutory objectives which are in the public interest, and must be active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data. The same criteria are set by Art 55 LED. Following these requirements, a more thorough description as to conditions for establishment of such an institution, way of recognition of their work in the public interest, etc. are required by the EU aquis. It would also be possible to list the named criteria and make a reference to a specific legislation that will regulate this area (for example a general association act).

In our opinion, since the Law lacs provisions in more detail on who can be a representative, it is questionable if the competence for representation will have only the appropriate/competent organisations.

Art 87:

The current law is unclear regarding how the criteria form Art 87 for punishing the violations, will be observed in the misdemeanour procedure. Art 87 of the Law uses the word 'administrative fines' (same as GDPR), when in the penalties section the word 'misdemeanour' is used. Since we are not expert in Serbian penal legislation, we would only like to point out that there is no clear indication that the criteria from Art 87 will be used in determining the penalty according to the procedure that will apply in individual case.

VIII. SPECIFIC PROCESSING SITUATIONS

Art 89:

The exercise of both human rights (access to public information and personal data protection) usually results in a conflict, so that the limitation of both rights is required to strike a fair balance in an individual case. In most cases, this balancing exercise cannot fully appreciate both human rights, so they must be adequately limited with regards to legitimate interests deriving from an individual case. Therefore, a more appropriate wording than 'achieved together' (which is used by Art 89 of the Law) would be 'fairly balanced' or 'appropriately balanced/observed'.

Art 91:

Paragraph 1, reads as follows: "For personal data protection in the field of labour and employment, provisions of the law governing labour and employment, as well as collective agreement, shall be implemented along with the provisions of this Law". The purpose of this provision should not be interpreted in a way that collective agreements may undermine or replace the requirements set by this law with regards to working relations. The purpose is to provide for a more specific rules to ensure the protection of rights and freedoms of individuals. The term 'along with' may not follow the outlined purpose. A better solution may be: 'in accordance with this law'.

For the same reason as commented above, Paragraph 2 also requires consideration for possible reappraisal, preferably according to the wording form Art 88 (2) GDPR: "Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of
personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the workplace.”

It should also be noted, that Art 91 does not fall under the scope of processing by competent authorities for special purposes, and this Art has no indication that it does not apply those types of processing.

Art 92:

As pointed out in general remarks the processing referred to in Art 92 also require for a special regulation. To specify this field of processing, a reference could be put down to the specific legislation or fields of legislation that implements such safeguards as stipulated in this article. The mentioned remark is not necessary for the alignment with the EU aquis, although it would facilitate the use of this Article in practice.

It should also be noted, that Art 92 does not fall under the scope of processing by competent authorities for special purposes, and that this Art has no indication that it does not apply to those types of processing.

Art 94:

There is no special exception provided by GDPR or LED to adopt a special regime as to data processing by public bodies for the purpose of collecting funds for humanitarian purposes.

Recital 46 GDPR states, that processing shall be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters. Bearing in mind the mentioned GDPR recital, raising funds for humanitarian actions cannot be considered the same purpose as processing of personal data for humanitarian purposes as set forth in recital 46. A general provision to allow the use of data by public bodies for the fundraising purposes from Art 94 is therefore not in conformity with data protection requirements laid down by GDPR or LED. This Art of the Law would be in line with GDPR if it referred to the use of data for the purposes set forth in recital 46 GDPR.

X. PENAL PROVISIONS

Art 95:

Sanctions are lacking for several provisions of this law, including processing without a legal base (Art. 12 of this Law), which is considered a major violation according to GDPR and such processing undermines the very foundations of data protection rules. Sanction is only provided for processing on the base of invalid consent (Art 15), which does not cover the scope of possible legal bases for processing. Also, the sanction for violation of Art 15 (conditions for consent) in our opinion is not adequately regulated (see next paragraph).

Para 1 item 5) refers to Art 15 of this Law which describes the conditions for a valid consent. The wording of the sanction provision (Art 95, Para 1, Item 5) does not adequately address the purpose of Art 15. Art 15 of the Law is intended to set up conditions for a valid consent. If the legislator wanted to incriminate the situation from Art 15, then this purpose has to be clearly outlined in the
sanction provision. A provision, such as for example: "...if he processes personal data, on the base of consent of the data subject that does not meet the requirements for a lawful consent according to this law (Art. 15)", or similar would better address the issue.
EXECUTIVE SUMMARY

There exists the necessity to consider amending Personal Data Protection Law of Serbia. Outlined below are some of the issues that require further examination and reconsideration.

LED IMPLEMENTATION:

Provisions regulating processing by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the prevention and protection of threats to public and national security (hereinafter: special purposes of processing) are scattered all over the Law, making it difficult to read and understand its aim and purpose. There is no clear indication to the issue of the scope of its application in regards to the application of LED. We suggest the Law to be clear and precise in determining that processing by competent authorities which is performed for purposes other than for the special purposes (prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public and national security), also falls under the scope of this Law and is governed by its (general) provisions. Such solution would, in our opinion, significantly contribute to the legal clarity and certainty of the Law and the legal security of data subjects. The Law should also provide for criteria for the storage limits (pay close attention to comment to Art 8).

RESTRICTIONS on RIGHTS OF DATA SUBJECTS have to be required by a special law (general remarks and comments to individual Articles: Art.28 Para 1, Art. 34 Para 2, Art. 40).

TRANSFERS:

Same standards should apply or/and a mechanism to approve transfers on the base of appropriate safeguards that were already approved according to EU law should apply (comments to Art 4. and 65). Also, tasks and competences should be revised in this respect (especially regarding SCC).

SPECIFIC PROCESSING SITUATIONS:

Article 94 requires special attention.

SANCTIONS:

It is inconclusive from this Law on how the conditions for administrative fines in individual cases will be observed according to the procedural legislation in play.

Also sanctions for many violations of general provisions are missing, including those that according to GDPR represent greater violation (eg. Processing without a legal base (art. 12), Violation of the rights of individuals, etc.).

OTHER:

In our opinion, it is not in contradiction with GDPR to regulate additional areas not covered by GDPR in the national law, if such need arises. In this respect the protection of personal data of deceased individual persons can be regulated. Furthermore, video surveillance, biometrics, records of entry to and exit from premises and other specific areas in order to avoid misinterpretation and legal uncertainty. The named institutes could be subject to a special chapter of the general law on data
protection or a separate law. Regulation of the named areas, though not subject to GDPR material, has proven in our practice to be useful.