REPUBLIC OF ALBANIA

RIGHT TO INFORMATION AND PERSONAL DATA PROTECTION COMMISSIONER

GUIDELINE

No.06, date 16.07.2025

ON
"ADOPTION OF THE METHODOLOGY FOR CALCULATING THE AMOUNT OF ADMINISTRATIVE SANCTIONS"

Pursuant to article 94 paragraph 4, article 85, paragraph 1, and article 97, paragraph 2 of Law no. 124/2024 "On Protection of Personal Data" (hereinafter referred to as "the *Law"*), the Information and Data Protection Commissioner, hereby issues the following,

GUIDELINE:

1. Determining the amount of administrative sanctions provided for in paragraphs1, 2 and 3 of article 94 of the Law, based on a specific assessment carried out on a case-by-case basis according to the text of the *"Methodology for Calculating the Amount of Administrative Sanctions",* attached to this Guideline.
2. The implementation of this Methodology, to enable a fair, transparent and proportional application of the calculation of the value of the administrative sanction measure.
3. The Information and Data Protection Commissioner's Office is responsible for implementing this Guideline.

This Guideline enters into force upon publication in the Official Gazette.

COMMISSIONER

Besnik Dervishi

METHODOLOGY

FOR CALCULATING THE AMOUNT OF

ADMINISTRATIVE SANCTIONS

CONTENT

EXECUTIVE SUMMARY

This Methodology for calculating administrative sanctions, adopted by the Information and Data Protection Commissioner's Office (hereinafter, "**the Commissioner's Office**"), constitutes a binding instrument for the General Directorate of Personal Data Protection at the Commissioner's Office, for a fair, transparent and correct assessment of the amount of administrative sanction against a certain controller/processor – infringer of the personal data protection legislation– as defined in article 94, in accordance with article 93, of Law no. 124, dated 19.12.2024 " *On Protection of Personal Data* " (hereinafter referred to as , "**the Data Protection Law**").

To support an assessment within the parameters provided for in the Data Protection Law, the Commissioner's Office has adopted this Methodology, **which consists of five steps**, for calculating administrative sanctions for infringements of its provisions.

First, the relevant data processing activity must be identified and the applicability of the provisions of paragraph 3 of article 93 (discussed in **Chapter 3** of this Methodology) shall be assessed.

Secondly, the starting point for calculating the amount of the administrative sanction must be identified **(Chapter 4)**. This is done by assessing the classification of the infringement under the provisions of the Data Protection Law, by assessing the degree of the infringement seriousness in light of the circumstances of the case, and by assessing the turnover of the undertaking/commercial company/non-profit organization according to the legal form of the controller/processor (hereinafter, "**Controller/Processor"**).

Thirdly, aggravating and/or mitigating circumstances related to the previous or current conduct of the controller/processor should be assessed, with a view to increasing or decreasing the sanction, in accordance with the relevant circumstances (**Chapter 5**).

Fourthly, the legal ceilings of the respective sanction amount for different infringements should be identified. The increases applied in the previous or subsequent steps cannot exceed this legal ceiling, as defined, respectively, in article 94, paragraph 1, 2 and 3 of the Data Protection Law (**Chapter 6)**.

Fifthly, it must be analyzed whether the final measure of the calculated sanction meets the requirements of its effectiveness, proportionality and preventive character. In any case, the relevant measure of the sanction may be subject to review in accordance with the circumstances of the case (Chapter **7)**, without exceeding in any case the legal ceilings for determining the measure of the sanction.

Throughout all the above-mentioned steps, it should be borne in mind that calculating the amount of the sanction is not a simple mathematical exercise. On the contrary, the circumstances of the specific case are the decisive factors that determine the final value of the sanction, which – in all cases – may vary between the minimum and maximum legal values.

CHAPTER 1 – INTRODUCTION

1.1 – Purpose

1. The purpose of this Methodology is to establish starting points for calculating the amount of the sanction, as an orientation, on the basis of which the calculation of the sanctions in practice for each specific case can be carried out. However, based also on EU case law, this Methodology cannot be so specific as to enable a given controller or processor to make a preliminary, precise, mathematical calculation of the expected sanction[1]. Throughout this document it is emphasized that the final sanction depends on all the circumstances of the specific case, which will be assessed on a case-by-case basis. Therefore, the Commissioner's Office aims for a harmonization approach as regards the existence of a model followed for calculating the amount of the sanction, rather than harmonizing the result of the calculation.

2. Notwithstanding this Methodology, the Commissioner's Office remains subject to all procedural obligations under the Albanian legislation in force, for the justification of the decisions taken, in the exercise of its supervisory/inspection activity. In this regard, although the Commissioner's Office must present sufficient legal arguments and reasons for its findings and conclusions, during the supervisory/inspection activity, in accordance with the provisions of the Albanian legislation in force, this methodology cannot and should not be interpreted as an exhaustive, precise and binding model for the Commissioner's Office to calculate the amount of the sanction or to predetermine the concrete impact of any aggravating or mitigating circumstances[2] of the case. Furthermore, a simple reference to this Methodology cannot replace the reasoning that must be provided in a specific case, in accordance with the procedural and substantive legislation in force.

3. This Methodology will be subject to continuous review, based on the practice of implementing the EU Regulation in EU countries, as well as based on the administrative practice of the Commissioner's Office.

[1] See, for example, Case C-189/02 P, C-202/02 P, C-205/02 P to C208/02 P and C-213/02 P, *Dansk Rørindustri A/S and Others v Commission,* paragraph 172 and Case T-91/11, *InnoLux Corp. v Commission,* paragraph 88.

[2] This is the *express position* of the European Data Protection Board, in the guidelines adopted by this Board regarding the calculation of administrative sanctions.

CHAPTER 2 – METHODOLOGY OF CALCULATING THE MEASURE OF ADMINISTRATIVE SANCTION

2.1 – General information

4. The calculation of the amount of the administrative sanction is at the discretion of the Commissioner's Office as the supervisory authority tasked by law for this purpose. The provisions and general spirit of the Data Protection Law require that the amount of the sanction in any individual case to be effective, proportionate and of preventive character (article 93 (1) of the Law). Furthermore, when determining the sanction amount, attention should be paid to the list of circumstances referring to the particularities of the infringement (its degree of importance) or the conduct of the offender (article 93 (2) of the Law). Therefore, the quantitative determination of the sanction measure is based on a specific assessment carried out in each case, taking into account the parameters included in the provisions of the Data Protection Law.

5. For conduct that violates data protection rules, the provisions of the Data Protection Law do not provide for a minimum sanction measure. On the contrary, they only provide for maximum ceilings, according to article 94 of the Law, in which several different types of conduct are grouped together. A sanction can be finally calculated, only by assessing and weighing all the elements expressly identified in paragraph 2 of article 93 of the Law, which are related to the relevant matter, as well as any other relevant element, whether or not expressly mentioned in the provisions in question (since the letter "gj" of paragraph 2 of article 93 of the Law requires that due regard be paid to any other applicable factor). Finally, the final sanction measure resulting from this assessment must be effective, proportionate and preventive character, for each specific case (paragraph 1 of article 93 of the Law). Any sanction imposed must take into account all the conditions provided for in this provision, but without exceeding the legal ceiling of the sanction measure, provided for in article 94 of the Data Protection Law.

2.2 - Synthesized overview of the Methodology

6. Taking into account these parameters, the Commissioner's Office has developed this Methodology for calculating administrative sanctions for infringements of the Data Protection Law.

Step 1:

Identification of processing processes/activities, according to the specific case and assessment of the application of paragraph 3 of Article 93 of the Data Protection Law (**Chapter 3)**.

Step 2:

Determining the model for further calculation of the sanction, based on an assessment of (**Chapter 4)**:

a) classification of the violation, according to paragraphs 1, 2 and 3, of article 94, of the Data Protection Law;
b) seriousness of the violation, according to letters "a", "b" and "e" of paragraphs 2, article 93, of the Data Protection Law;
c) turnover of the enterprise, as an important element to be taken into consideration, with the aim of imposing an effective, proportionate and preventive character sanction, as per paragraph 1 of article 93, of the Data Protection Law.

Step 3:

Assessment of aggravating and mitigating circumstances related to the previous or current conduct of the controller/processor and the increase or decrease of the sanction, in accordance with these circumstances (**Chapter 5**).

Step 4:

Identification of the legal ceiling for the sanction amount related to the various processing processes/activities. The increases applied or to be applied cannot exceed this ceiling (**Chapter 6**).

Step 5:

Conducting an analysis of whether the final amount of the calculated sanction meets the requirements of effectiveness, proportionality and deterrence, as required by the provisions of point 1, of 93, of the Data Protection Law, and increasing or decreasing the amount of the sanction, accordingly (**Chapter 7**).

2.3 – Violations punishable by fixed measures

7. In certain circumstances, the Commissioner's Office may consider that certain violations may be punished with an administrative sanction in a predetermined amount. It is at the discretion of the Commissioner's Office to determine which types of infringements qualify as such, based on their nature, importance and duration.

8. Fixed measures of administrative sanctions may be determined at the discretion of the Commissioner's Office, taking into account - among other things - the circumstances and the social and economic situation in the country, in relation to the seriousness of the violation, in accordance with letters "a", "b" and "e" of paragraph 2 of article 93 of the Data Protection Law.

CHAPTER 3 – CONCURRING INFRINGMENTS AND APPLICATION OF ARTICLE 93(3) OF THE LAW

9. Before calculating the amount of a sanction based on this Methodology, it is important to first consider what conduct (the factual circumstances surrounding the conduct) and infringement (the abstract legal description of the sanctionable action) the sanction is based on. In practice, a particular case may include circumstances that may be considered:

    (i) as one sanctionable conduct; or
    (ii) as several specific sanctionable conducts.

    It is also possible that a single conduct may give rise to a number of different infringements, which may be mutually exclusive or may coexist with each other. In other words, there may be cases of competing/simultaneous infringements. Depending on the concurrence rules, these infringements may lead to different calculation of sanctions.

10. Based on the case law of the European Court of Justice, concerning the rules on concurrent infringement cases, and taking into account the different purposes of their application and legal consequences, these principles can be grouped roughly into three categories as follows:

    - Concurrence of infringements (Subchapter **3.1.1)**.

    - Unity of action (Subchapter **3.1.2)**,

    - Multiple actions (Chapter **3.2)**.

11. These different categories of concurring do not conflict with each other, but have different areas of application and fit into a coherent overall system, providing for a logical testing scheme.

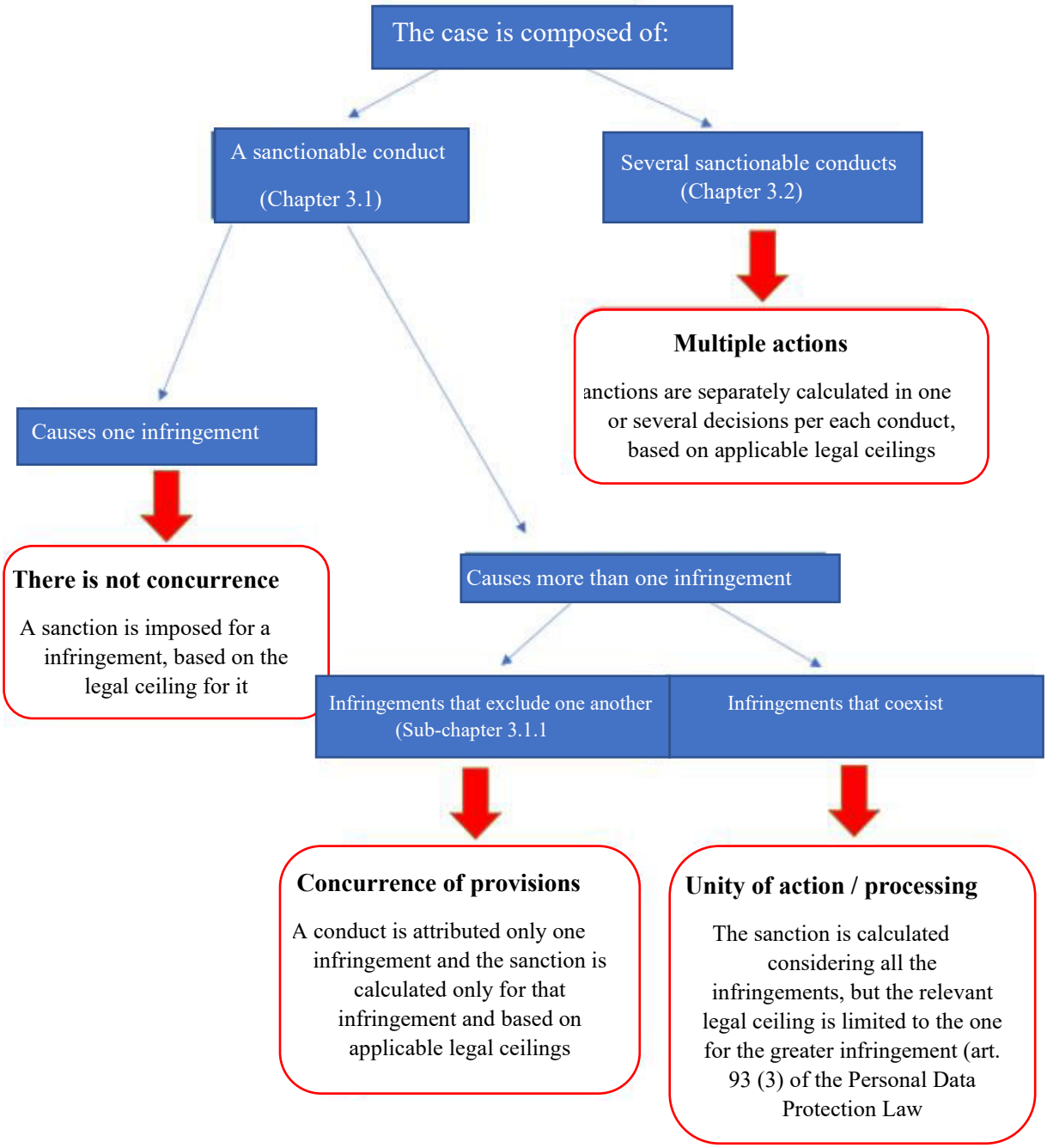
12. Therefore, it is important to first determine:

a. Whether the circumstances should be considered as one sanctionable conduct (Chapter **3.1)** or multiple sanctionable conducts (**Chapter 3.2)**;

b. In the case of sanctionable conduct (Chapter **3.1)**, whether or not this conduct constitutes one or more infringements; and

c. In the case of conduct that gives rise to multiple infringements, the attribution of one infringement excludes the attribution of another infringement (**Subchapter 3.1.1)** or if they coincide, they are subordinate to each other (**Subchapter 3.1.2)**.

DIAGRAM:


The case is composed of:
A sanctionable conduct
(Chapter 3.1)
Several sanctionable conducts
(Chapter 3.2)
Multiple actions
anctions are separately calculated in one or several decisions per each conduct, based on applicable legal ceilings
Causes one infringement
There is not concurrence
A sanction is imposed for a infringement, based on the legal ceiling for it
Causes more than one infringement
Infringements that exclude one another
(Sub-chapter 3.1.1
Infringements that coexist
Concurrence of provisions
A conduct is attributed only one infringement and the sanction is calculated only for that infringement and based on applicable legal ceilings
Unity of action / processing
The sanction is calculated considering all the infringements, but the relevant legal ceiling is limited to the one for the greater infringement (art. 93 (3) of the Personal Data Protection Law

3.1 - Sanctionable conduct

13. As a first step, it is essential to determine whether there is a sanctionable conduct, or several ones, in order to identify the relevant sanctionable conduct that will be subject to the sanction. It is therefore important to understand which circumstances are considered to be one and the same conduct, as opposed to multiple conducts. The relevant sanctionable conduct must be assessed and identified on a case-by-case basis. For example, in a given case, identical or related data processing processes/activities may constitute one (same) conduct.

14. The term "*processing process/activity"* is included in paragraph 16, article 5, of the Data Protection Law, where " *processing* " is defined as " *any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, dissemination by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.* "

15. When assessing "*the same or related processing operations/processes*", it should be borne in mind that the Commissioner's Office may take into account, for the assessment of infringements, all legal provisions that oblige the lawful performance of processing operations/processes, including for example, transparency obligations (e.g. article 13 of the Data Protection Law). This is also emphasized by the phrase "*for the same or related processing operations/processes*", which indicates that the scope of this provision includes any infringement that is related to and may have an impact on the same or related processing operations/processes.

16. The term "*connected*" refers to the principle according to which a unitary/single conduct may consist of several parts carried out by a unitary/same will and are connected (in particular as regards the identity of the data subject, the purpose and the nature of the processing), in space and time, so closely that an external observer would consider them to be a coherent conduct. In order to apply the principles, prevent infringements and effectively enforce the law, it is important to presume the existence of a sufficient connection between the processing operations/activities. Therefore, these aspects of the relationship for a sufficient connection between the processing operations/activities must be assessed on a case-by-case basis.

Example 1a – Same or related processing processes/activities

A financial institution requests a credit reporting agency (CRA) to perform a creditworthiness check on a particular borrower. The financial institution receives this information and stores it in its system.

Although the collection and storage of creditworthiness data by the financial institution each constitute a processing operation/activity in itself, they form a group of processing operations/activities that are carried out with the same intent and are connected, in space and time, in such a close way to each other that an external observer would consider them to be a single conduct. Therefore, the processing operations/activities carried out by the financial institution must be considered as "connected" and constitute the same conduct.

Example 1b – Same or connected processing processes/activities

A data intermediary decides to undertake a new processing activity: it decides to collect – as a third party – the history of customer transactions from dozens of retailers, without a legal basis for this, in order to perform psychometric analyses to predict the future behavior of individuals, including their political voting behavior/bias/affiliation, willingness to leave their jobs, etc. In the same decision, the data intermediary decides not to record this procedure in the logs of processing activities, not to inform data subjects and to ignore any request for their access regarding the new processing operations.

The processing operations included in this processing operation form a series of processes/processing activities carried out with a unitary/same intention and are linked in space and time. They should be considered as "linked" and forming the same conduct. This also includes the failure to record the processing activity in the relevant registers, the failure to inform data subjects and the failure to establish procedures to respect the right of access in relation to new processing operations. These obligations have been infringed for the linked processing processes/activities.

Example 1c – Different and independent processing processes

(i) A controller in the area of construction conducts a background check on a job candidate. The background check also includes political affiliation, union membership, and sexual orientation.

(ii) Five days later, the entity in question requests from its contractors (individual traders) an excessive self-declaration regarding their business agreements with other parties, despite the fact that this is not related to the contract in force between them or the legal compliance obligations, defined by the legislation of the field.

(iii) A week later, the controller in question becomes subject to a data breach (leaks loss) of the data processed by it. The controller's network is hacked – despite having appropriate technical and organizational measures in place – and the hacker in question gains access to a system that processes the personal data of citizens who have submitted requests to the controller in question. Despite the fact that the data was appropriately encrypted in accordance with applicable standards, the hacker is able to break it using military-grade encryption technology and sells the data on the dark web. The construction entity does not notify the Commissioner's Office of the data breach in question, despite its obligation to do so.
The processing processes/activities in this case, i.e. the background check of the job candidate, the self-declaration requirements to contractors and the failure to notify the Commissioner's Office of the personal data breach, are not connected in themselves. Therefore, they should not be considered as "linked" processes/activities, but, on the contrary, they constitute different (not the same) conduct.

17. Where it is found that the circumstances of the case constitute the same conduct and give rise to a single infringement, the sanction may be calculated on the basis of that offence and the legal threshold for the amount of sanction. However, where the circumstances of the case constitute the same conduct but this conduct gives rise to not just one but several infringements, it must be established whether those infringements are mutually exclusive (Sub-chapter 3.1.1), or whether they are cumulative/subordinate to each other (Chapter 3.1.2). Where the circumstances of the case constitute multiple conduct, they must be considered as a set of actions and treated in accordance with Chapter 3.2.

3.1.1 - Concurrence of infringements

18. The principle of concurrence of infringement[3] is applicable in any case where the application of one provision of the law excludes or absorbs the application of another provision. In other words, concurrence already occurs at the abstract level of the legal provisions. This can occur based on the principle of specialty, subsidiarity or consumption, which are often applicable when the provisions of the law protect the same legal interest. In such cases, it would be unlawful to impose sanctions on the offender twice for the same infringement.

19. In the case of concurring infringements, the sanction measure should be calculated only on the basis of the violation identified according to the above rules (the predominant violation).

The principle of specialty

20. The principle of *lex specialis* (*specialia generalibus derogant*) is a legal principle that implies that a more specific provision (derived from the same legal act or different legal acts of the

[3]Also referred to as "*apparent concurrence*" or "*false concurrence"*.

same legal force) supersedes a more general provision, even though both pursue the same objective. The more specific infringement is sometimes considered a "qualified type" of infringement compared to the less specific one. The qualified type of infringement may be subject to a higher level of sanction, a higher legal ceiling or a longer limitation period.

21. However, sometimes, through the technique of interpretation, the principle of *lex specialis* can also be applied in cases where, due to its nature and systematics, an infringement is considered as qualifying another significantly more specific infringement, although its wording does not explicitly mention an additional element.

22. When two provisions pursue different objectives from each other, this constitutes a differentiating factor that justifies the imposition of separate sanctions. For example, if an infringement of one provision automatically results in an infringement of the other, but the reverse does not occur, these violations pursue different objectives.

23. The principle of *lex specialis* can only be applied if and to the extent that the objectives pursued by the respective infringements are in fact similar in the individual case. Since the data protection principles, as set out in article 6 of the Data Protection Law, are defined as comprehensive concepts, there may be situations where other provisions are a concretization of this principle, but do not limit the principle in its entirety. In other words, a provision does not always determine the full scope of the principle. Therefore, depending on the circumstances, in some cases they overlap in a similar way and one infringement may replace the other, while in other cases the overlap is only partial and therefore not entirely the same. As long as they are not similar, there is no overlap of infringements. Instead, they can be considered alongside each other in the context of calculating the sanction.

The principle of subsidiarity

24. Another form of concurrence of offences is often referred to as the principle of subsidiarity. It applies if an offence is considered to be subsidiary to another offence. This can happen either because the law formally provides for subsidiarity or because subsidiarity exists for material reasons. The latter may be the case where the infringements have the same objective, but one carries a lesser gravity in relation to the other (e.g. an administrative offence may be subsidiary to a criminal offence, etc.).

The principle of consumption

25. The principle of consumption applies in cases where the infringement of one provision leads to the infringement of another, often because one infringement precedes the other.

3.1.2 – Unity of action - Article 93(3) of the law

26. Similar to the situation of concurrence of infringements, the principle of unity of action[4] applies in cases where a conduct is subject to regulation by several legal provisions, with the difference that no provision is excluded and is not absorbed by the other, because they do not fall under the same legal provision, because they do not fall in the field of implementing the principles of specialty, subsidiarity or consumption and, most of all, pursue different objectives.

27. The principle of unity of action is specified in paragraph 3 of article 93 of the Data Protection Law in the form of a "*unity of processing*". It is important to understand that paragraph 3 of article 93 of the Data Protection Law is limited in its application and will not apply to every case in which it is found that multiple infringements have occurred, but only to those cases where the multiple infringements have resulted from the same, or related, processing processes/activities as explained above. In these cases, the total amount of the administrative sanction shall not exceed the amount specified for the most serious infringement.

28. If a controller or processor has infringed the provisions of the Data Protection Law, deliberately or by negligence, for the same or related processing operations/activities, the total amount of the sanction shall not exceed the amount for the most serious infringement (article 93(3) of the Law).

29. In some special cases, a unity of action may also be assumed, where a single action infringes the same legal provision several times. This may be the case in particular where circumstances give rise to a repeated and similar infringement of the same legal provision in close continuity in space and time.

> ***Example 2 – Unity of action***
>
> *A controller sends a multitude of marketing emails to different groups of data subjects, at different frequencies throughout the day, without having a legal basis and thus infringes, with unity of action, paragraph 1 of article 7 of the Data Protection Law several times.*

30. The content of paragraph 3 of article 93 of the Data Protection Law does not seem to directly cover this last case of unity of action, since it does not appear that "*several provisions of the law*" have been infringed. However, it would constitute unequal and unfair treatment if an offender, who by one act infringes different provisions pursuing different objectives, were to be privileged over an offender who by the same act infringes the same provision pursuing the same objective several times. In order to avoid inconsistency of the legal principle and to

[4]Also referred to as "*ideal concurrence*".

respect the fundamental right to equal treatment, paragraph 3 of article 93 of the Data Protection Act will be applied *mutatis mutandis in such cases*.

31. In the event of a single action, the total sanction amount must not exceed the applicable legal ceiling for the most serious infringement. Regarding the interpretation of paragraph 3 of article 93 of the Data Protection Law, it is worth noting that, based on the principle of interpreting the norm according to its purpose (*effet utile*) – in determining the sanction amount – this provision should not be interpreted in a way that relativizes the fact whether the offender has committed one or more infringements of the Data Protection Law.

32. The term "*total measure*" implies that all violations committed must be taken into account when assessing the measure of the sanction/amount of sanction and the phrase "*amount foreseen for the most serious infringement*" of paragraph 3 of article 93 refers to the legal ceilings of sanctions (according to article 94 of the Law). Therefore, although the sanction itself cannot exceed the legal ceiling of its highest level, when assessing the measure of the final sanction, the offender will nevertheless be considered expressly guilty of infringing several provisions and these infringements must be taken into account for this purpose.

3.2 – The multiple sanctionable actions

33. The principle of multiple actions[5] describes all cases that are not included in the principles of concurrence of infringements (Subchapter 3.1.1) or in paragraph 3 of article 93 of the Law on Personal Data Protection (Subchapter 3.1.2).

34. The only reason why these infringements are dealt with in a single decision is that they coincidentally come to the attention of the inspectors of the Commissioner's Office at the same time, without being identical or related processing operations within the meaning of paragraph 3 of article 93 of the Data Protection Law. Therefore, in this case, it is established that the offender has infringed several legal provisions and is administratively sanctioned with separate sanctions in the same decision or in separate decisions of the Commissioner. Furthermore, since paragraph 3 of article 93 of the Data Protection Law does not apply, the total amount of the sanction may exceed the amount specified for the most serious infringement (*argumentum e contrario*). Cases of multiple actions do not constitute any reason to privilege the offender with regard to the calculation of the amount of the sanction. However, this does not affect the obligation to respect the general principle of proportionality.

[5]Also referred to as "*real concurrence*", "*factual concurrence*" or "incidental *concurrence*".

Example 3 – Multiple actions

After carrying out a data protection inspection at the premises of a controller, the Commissioner's Office finds that the controller has not provided for any procedure for the continuous review and improvement of the security of its website, for providing employees with the information of Article 13 of the Law regarding the processing of human resources data and for informing the Commissioner's Office of a recent data breach of data processed/collected by its contractors. None of the breaches are excluded from, or included in, each other on the basis of lex specialis, subsidiarity or consumption. Furthermore, they do not qualify as the same processing activity or linked processing activity; thus, they do not constitute a unity of action, but a plurality of actions. Therefore, the Commissioner's Office will find various breaches of articles 13, 28 and 29 of the Data Protection Law. For this reason, the controller will be sanctioned with individual sanctions for each infringement, without being limited by a single legal ceiling applicable to their amount.

CHAPTER 4 – STARTING POINT FOR CALCULATING THE AMOUNT OF ADMINISTRATIVE SANCTION

35. The Commissioner's Office considers that the calculation of the amount of sanction should start from a certain starting point [6]. This starting point constitutes the starting point for the further calculation of the sanction, where all the circumstances of the case are taken into account and assessed, resulting in the final sanction amount to be imposed on the controller and/or processor concerned.

36. The identification of the starting point for calculating the amount of the sanction does not affect the decision-making of the Commissioner to take into account the relevant circumstances of each case of infringement. The sanction imposed on a controller/processor may range from the minimum measure up to the ceiling provided for by law, provided that this administrative sanction is effective, proportionate and of a preventive character. The existence of a starting point does not prevent the Commissioner from increasing the amount of the sanction (up to the legal ceiling), if the circumstances of the case so require.

37. The Commissioner's Office considers three essential elements in determining the starting point for calculating the sanction:

    (i) categorizing infringements according to their nature, according to article 94 of the Data Protection Law,

[6]The Court of Justice generally accepts that calculations start from an abstract starting point. In particular in Joined Cases C-189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P, Dansk Rørindustri, but also in more recent cases such as Case T-15/02, BASF AG v Commission, paragraphs 120-121; 134, Case C-227/14 P, LG Display Co. Ltd v Commission, paragraph 53 and Case T-26/02, Daiichi Pharmaceutical Co. Ltd v Commission, paragraph 50.

(ii) the degree of importance of the infringement, based on article 93 paragraph 2 of the Data Protection Law, as well as

(iii) the turnover of the enterprise, which are taken into consideration, with the aim of imposing an effective, proportionate and dissuasive sanction, based on article 93 paragraph 1 of the Data Protection Law. These elements are explained in Chapters 4.1, 4.2 and 4.3 below.

4.1 - Categorization of infringements according to article 94 of the Law

38. Almost all obligations of controllers and processors are categorized, according to their nature, in the provisions of article 94 of the Personal Data Protection Law, where two categories of infringements are foreseen: (i) infringements punishable under paragraph 1 of article 94 and (ii) infringements punishable under paragraphs 2 and 3 of article 94. The first category of infringements is punishable by a sanction of up to 1 000 000 000 ALL or 2% of the annual turnover for the previous financial year of the controller/processor, whichever is higher. While the second case is punishable by a sanction of up to 2 000 000 000 ALL or 4% of the annual turnover for the previous financial year of the controller/processor, whichever is higher.

39. With this distinction, the legislator has defined the first indicator of the degree of importance of an infringement in the abstract sense. The more serious the violation, the greater the sanction may be**.**

4.2 - The degree of seriousness of the infringement according to the circumstances in each individual case

40. The Personal Data Protection Law also provides that the circumstances that qualify the seriousness of the infringement in an individual case must be taken into account. In other words, the Law requires the Commissioner's Office of the to take into account the nature, importance and duration of the infringement, considering the nature, object or purpose of the processing concerned, as well as the number of data subjects affected by the infringement and the level of damage caused to them (article 93(2)(a) of the Law); the intentional character (intention) or negligence (article 93(2)(b) of the Law); and the categories of personal data affected by the infringement (article 93(2)(e) of the Law).

41. The Commissioner's Office analyses these elements in light of the circumstances of the case in question and concludes – on the basis of this analysis – as to the degree of seriousness of the infringement (as will be discussed below, in paragraph 49). In this context, the Commissioner's Office may also take into account whether the relevant data was directly identifiable. Although they are treated individually in this Methodology, in practice these elements are often intertwined and must be seen in relation to the facts of the case as a whole.

4.2.1 - Nature, significance and duration of the infringement

42. Article 93, paragraph 2, letter "a" of the Personal Data Protection Law has a broad scope and requires the Commissioner's Office to conduct a full examination of all the elements constituting a particular infringement, which are sufficient to differentiate it from other infringements of the same type. This assessment must take into account the following specific elements:

a) **The nature of the infringement,** assessed on the basis of the specific circumstances of the case. In this sense, this analysis is more specific than the abstract classification of paragraphs 1, 2 and 3 of article 94 of the Law. The Commissioner's Office may also take into account the interest that the provision infringed aims to protect and its place in the framework of the personal data protection. The Commissioner's Office may also take into account the extent to which the infringement in question has impeded the effective implementation of the provision and the achievement of the objective that it aims to protect;

b) **The significance of the infringement,** assessed on the basis of the specific circumstances of the case. As defined in letter "a" of paragraph 2, of article 93 of the Law. Indicators of the significance of the breach are the nature of the processing, but also its object and purpose, as well as the number of data subjects affected and the level of damage caused to them.

   i. **The nature of the processing,** including the context in which the processing is carried out (e.g. business activity, non-profit activity, political party, etc.), as well as all the characteristics of the processing. Where the nature of the processing entails higher risks, e.g. where the purpose is to monitor behaviors, evaluate personal aspects or take decisions or measures with adverse effects on data subjects, depending on the context of the processing and the role of the controller or processor, the Commissioner's Office may consider giving more weight to this factor. It may also be important to assess this factor where the data subject and the controller are in an unequal position (e.g. where the data subjects are employees, students or patients) or where the processing involves a vulnerable category of data subjects, in particular children/minors.

   ii. **The object of the processing,** based on the domestic or cross-border object of the processing carried out and the relationship between this information and the actual scope/extent of the processing, having regard to the resources allocated for this purpose by the controller. This element highlights a real risk factor, linked to the increasing difficulty for the data subject and the Commissioner's Office to deter unlawful conduct as the object of the processing increases. The larger the object of the processing, the more weight the Commissioner's Office may give to this factor.

   iii. **The purpose of the processing** is a factor that the Commissioner's Office attaches great weighting to, also considering whether the purpose (of the processing) constitutes the so-called "*core activity"* of the controller. The more central the

processing is to the core activities of the controller or processor, the more serious the irregularities in that processing will be. In such circumstances, this factor takes on greater importance/weight. However, there may be circumstances in which the processing of personal data no longer constitutes a core activity of the controller or processor, but significantly affects the assessment (this is the case, for example, of processing relating to the personal data of employees, where the infringement significantly affects their dignity).

iv. **Number of data subjects** actually or potentially affected. The greater the number of data subjects involved; the more weight the Commissioner's Office may give to the assessment of this factor. In many cases, it may also be considered that the infringement gains a systemic/widespread nature and may therefore affect, at different times, other data subjects who have not lodged a complaint with the Commissioner's Office. The Commissioner's Office may, depending on the circumstances of the case, take into account the ratio between the number of data subjects affected and the total number of data subjects in that context (e.g. the number of citizens, customers or employees) in order to assess whether the infringement is of a systemic nature.

v. **The level of harm** suffered and the extent to which the conduct may affect individual rights and freedoms. For this reason, the reference to the "*level"* of harm suffered is intended to draw the attention of the Commissioner's Office to the harm caused, or which could have been caused, as a separate parameter, in relation to the number of data subjects involved (e.g., in cases where the number of individuals affected by the unlawful processing is large, but the harm suffered by them is marginal/secondary). The level of harm suffered refers to physical, material or non-material damage [7]. The assessment of harm is, in any case, limited to what is functionally necessary to achieve an accurate assessment of the degree of importance of the infringement, as indicated in paragraph 49 below, without creating overlap with the activity of the judicial authorities tasked with ascertaining the various forms of individual harm.

c) **The duration of the infringement**, which means that the Commissioner's Office may give more weight to an infringement of greater duration. If a certain conduct was illegal under the previous regulatory framework, both the period after the date of entry into force of the new Law and the previous period may be taken into account in determining the measure, in each case, taking into account the provisions of the previous legal framework.

43. The Commissioner's Office may give weight to the above-mentioned factors, depending on the circumstances of the case. If they do not have particular weight in a specific case, they may not be taken into consideration in the case.

[7]See recital 75 of the EU Regulation.

4.2.2 – Deliberate character (intent) or negligence

44. In EU practice, in the data protection area, as well as based on the position of EDPB in general in general, "*intention*" includes both (malicious) knowledge and will regarding the characteristics of an infringement, while the term "*unintentional*" implies that there was no intention to cause an infringement despite the controller/processor has infringed the "*duty of diligence"* required by law [8]. Unintentional, in this sense, is not equivalent to involuntary.

Example 4 – Illustrations of intent and negligence, according to the EDPB

Circumstances indicating intentional infringement may include unlawful processing expressly authorized by the controller's senior management/directors or against advice from the data protection officer, or in disregard of existing policies – for example, obtaining and processing data about a competitor's employees with the aim of discrediting that competitor in the market. Other examples here could be:

- *changing personal data to distort facts (with the aim of giving a false positive impression) regarding the fulfillment of objectives;*

- *the trading of personal data for marketing purposes, i.e. selling data as "opted in", without checking/ignoring the will of the data subjects on how their data should be used.*

Other circumstances, such as failure to read and comply with existing policies, human error, failure to check personal data in published information, failure to implement technical updates in a timely manner, failure to approve policies (rather than failure to implement them) may be indicators of negligence.

45. The intentional or negligent nature of the infringement (article 93(2)(b) of the Law) must be assessed by taking into account the objective elements of conduct gathered from the facts of the case. As stated by the EDPB "it *is generally accepted that intentional infringements, which show disregard for the provisions of the law, are more serious than unintentional ones.*" [9] Thus, in the case of an intentional infringement, the Commissioner's Office may attach greater importance to this circumstance. Depending on the circumstances of the case, the Commissioner's Office may also attach importance to the degree of negligence, which, at best, may not be taken into account in the case.

4.2.3 - Categories of affected personal data

46. Regarding the requirement to take into account the categories of affected personal data (article 93(2)(e) of the Law), the Personal Data Protection Law clearly highlights the types of data that

[8]See the guidelines of the Working Party 253 (WP253) of the EDPB, p. 11.
[9]See the guidelines of the EDPB Working Group 253 (WP253), p. 12.

deserve special protection and, consequently, stricter treatment in the context of the application of sanctions measures. This concerns the types of data provided for in the provisions of articles 9 and 10 of the Personal Data Protection Law, of as well as data outside the scope of these articles, which dissemination causes immediate damage or inconvenience to the data subject (e.g., location data, private communication data, personal identification numbers or financial data, such as transaction statements or credit card numbers) [10]. In general, the more such categories of data are involved, or the more sensitive the data, the more importance is given to this factor.

47. Furthermore, the amount of data relating to each data subject involved in a processing activity is important, as the infringement of the right to privacy and protection of personal data increases proportionally with the amount of data processed for each data subject.

4.2.4 - Classification of the importance of the infringement and identification of the starting amount for calculating the administrative sanction

48. The assessment of the above factors (according to Sub-chapters 4.2.1 - 4.2.3) determines the significance of the infringement as a whole. This assessment does not consist of a mathematical calculation, in which the above-mentioned factors are taken into account individually, but in a complete assessment of the concrete circumstances of the case, in which all the above-mentioned factors are interconnected. Therefore, in examining the significance of the infringement, attention must be paid to the infringement as a whole.

49. Based on the assessment of the above factors, the Commissioner's Office may determine that the infringement is of a low, medium or high degree of importance. These categories do not affect whether or not a sanction may be imposed.

- When calculating the amount of the sanction for a violation of a low degree of importance, the Commissioner's Office sets the starting point for further calculation at a value between 0 and 10% of the applicable legal ceiling.
- When calculating the amount of the sanction for a violation of a medium degree of importance/, the Commissioner's Office sets the starting point for further calculation at a value between 10 and 20% of the applicable legal ceiling.
- When calculating the amount of the sanction for an infringement of a high degree of importance, the Commissioner's Office sets the starting point for further calculation at a value between 20 and 100% of the applicable legal ceiling.

[10]The dissemination of private communications and location data may cause immediate harm or inconvenience to the data subject, which has been highlighted by the specific protection granted by the EU legislator to private communications in Article 7 of the Charter of Fundamental Rights and Directive 2002/58/EC, as well as by the ECJ to location data in certain cases, see Joined Cases C-511/18, C-512/18 and C-520/18, La Quadrature du Net et al, paragraph 117 and the case-law cited there.

50. As a general rule, the more serious the infringement within its category, the higher the starting point of the calculation is likely to be.

51. The ranges within which the respective starting points of the calculation are determined remain, however, at the further discretion of the Commissioner's Office and may be adjusted at its sole discretion, if and when necessary.

Example 5a – Qualification of the importance of an infringement (high degree of importance)

After investigating numerous complaints about unsolicited phone calls, from customers of a telephone operator, the Commissioner's Office found that the controller in question was using the contact details of its customers for telemarketing purposes, without a valid legal basis (violation of article 7 of the Personal Data Protection Law). Specifically, the telephone operator had provided third parties with the names and registered telephone numbers of its customers for marketing purposes. This controller had done so despite the advice/recommendations of the Data Protection Officer against such processing, without making any effort to curb the practice or to offer customers a way to object to this processing. In fact, this practice had started in February 2025 and was still ongoing at the time of the investigation. The controller in question operated nationwide and the practice affected all of its 1 million customers. The Commissioner's Office found that all of these customers had been regularly subjected to unsolicited calls from third parties, with no effective means of stopping them.

The Commissioner's Office was required to assess the significance of this case. As a starting point, the Commissioner's Office noted that an infringement of article 7 of the Personal Data Protection Law is listed among the infringements provided for in article 94, paragraph 2 of the Law and, therefore, it is categorized at the highest level of breach provided for by this article. Secondly, the Commissioner's Office assessed the circumstances of the case. In this regard, the Commissioner's Office attached great importance ***to the nature of the infringement****, since the infringed provision (article 7 of the Law) supports the lawfulness of data processing as a whole. Failure to comply with this provision undermines the lawfulness of the processing as a whole. The Commissioner's Office also attached great importance* ***to the duration of the infringement****, which began with the entry into force of the Law and had not ceased by the time of the investigation. The fact that the controller operated at a national level gave importance to the object of the processing.* ***The number of data subjects*** *involved was considered very high (1 million, compared to a total population of 3 million inhabitants), while* ***the degree of damage suffered*** *by them was considered moderate (non-material damage, in the form of inconvenience/nuisance). This assessment was carried out taking into account* ***the categories of data affected*** *(name and telephone number). However, the importance of the infringement was increased by the fact that it was carried out in contravention of the advice of the data protection officer and was therefore considered to be* ***intentional/deliberate****.*

Taking into account all of the above (serious nature, long duration, large number of data subjects, nationwide scope, deliberate nature, against a moderate damage), the Commissioner's Office concluded that the breach is considered to be of a high degree of importance. For this reason, as a starting point for calculating the amount of the sanction, the Commissioner's Office set a value between 20% and 100% of the legal ceiling, provided for in article 94, paragraph 2 of the Personal Data Protection Law.

Example 5b – Qualification of the importance of an infringement (average degree of importance)

The Commissioner's Office received a notification of a personal data breach from a hospital. From this notification, it emerged that some staff members had been able to access (see) parts of patients' health records that – given the pavilion where they worked – should not have been accessible to them. The hospital was working on defining procedures governing access to patient record files and had implemented strict access restrictions. This meant that staff on a pavilion could only access medical information related to that specific pavilion. In addition, the hospital had invested in raising awareness of the importance of privacy among its staff members. However, as the administrative investigation revealed, the hospital had problems with monitoring access authorizations to the processed data. Staff members who were transferred between pavilion were still able to access the records of patients admitted to their previous pavilion and the hospital had no procedures in place to match the staff member's current position with their authorization. The hospital's internal investigation found that at least 150 staff members (out of 3,500) had incorrect authorizations, affecting at least 20,000 out of 95,000 patient record files. The hospital was able to prove that, on at least 16 occasions, staff members had used their authorizations to view patient record files. The Commissioner's Office found that there had been a breach of article 28 of the Personal Data Protection Law.

In assessing the significance of the breach in this case, the Commissioner's Office initially noted that a breach of article 28 of the Personal Data Protection Law is classified as a breach of article 94(1) of the Law and, therefore, is ***categorized under the mildest sanction under that Article****. Secondly, the Commissioner's Office assessed the circumstances of the case. In this regard, the Commissioner's Office considered that although* ***the number of data subjects*** *affected by the infringement was only 16, potentially this number could have been 20,000 based on the circumstances of the case up to, even, 95,000, given the systemic nature of the case. The Commissioner's Office further categorized the infringement as* ***negligence****, but not of major importance, which was considered to be an irrelevant factor in the circumstances of this particular case, due to the fact that the hospital had not adopted authorization policies, which it certainly should have done, but had, on the other hand, taken steps to implement strict measures to limit access. This assessment was not affected by the fact that other data protection and security policies were successfully implemented, as required by the provisions of the Personal Data Protection Law. Finally, the Commissioner's Office attached great*

*importance to the fact that the patient files contained health data, which are **sensitive data,** according to article 9 of the Personal Data Protection Law.*

*Taking into account all of the above (the nature of the processing and the fact that the data were sensitive, against the number of data subjects actually and potentially affected, the Commissioner's Office concluded that the breach is considered to be of a **medium degree of importance**. The Commissioner's Office set as the starting point for the further calculation of the sanction a value between 10 and 20% of the legal ceiling provided for in paragraph 1, of article 94 of the Personal Data Protection Law.*

Example 5c – Qualification of the importance of an infringement (low degree of importance)

The Commissioner's Office has received numerous complaints about the way an online store handles the right of data access of its subjects. According to the complainants, the handling of their requests for access took between 4 and 6 months, which is outside the time limit allowed by the provisions of the Personal Data Protection Law. The Commissioner's Office investigated the complaints and found that the online store responds to requests for access, at most, 3 months late in 5% of cases. In total, the store had received around 1000 access requests on an annual basis and confirmed that 950 of them were handled on time. Furthermore, the online store had adopted policies to ensure that all requests were handled correctly and completely. However, the Commissioner's Office concluded that the online store had violated paragraph 4, of article 12, of the Personal Data Protection Law and sanctioned this infringement with a fine.

*When calculating the amount of sanction, the Commissioner's Office assessed the degree of importance of the infringement in this case. Regarding the starting point of the calculation, the Commissioner's Office observed that the case in question resulted in an infringement of article 12 of the Personal Data Protection Law, **which is listed among the sanctionable infringements under paragraph 2 of article 94 of the Personal Data Protection Law**, which constitutes the highest level of the sanction provided for by this article. Secondly, the Commissioner's Office assessed the circumstances of the case. In this regard, it carefully analyzed **the nature of the infringement**. Although the right to access personal data, within the time limits of the law, is one of the foundations of the rights of the data subject, the Commissioner's Office considered that the violation was of a limited importance, since all requests had been dealt with definitively and with a limited delay. Taking into account **the purpose of the processing,** the Commissioner's Office found that the processing of personal data was not the core activity of the online store, but nevertheless an important auxiliary means in fulfilling its objective of selling goods online. The Commissioner's Office took this into account to reduce the level of significance of the infringement. On the other hand, **the level of harm** suffered by data subjects was considered minimal, as all access requests were handled within 6 months.*

Taking into account all of the above (the nature of the infringement, the purpose of the processing and the degree of damage), the Commissioner's Office concluded that the

infringement is of a low level of importance. The Commissioner's Office set as the starting point for calculating the amount of the sanction a value between 0 and 10% of the legal ceiling provided for in point 2 of article 94 of the Personal Data Protection Law.

4.3 - Enterprise turnover as an element for imposing an effective, proportionate and preventive character sanction

52. The law requires the Commissioner's Office to ensure that the administrative sanction (fine) is effective, proportionate and with preventive character in each individual case (article 93(1) of the Law). The application of these principles of the law may have far-reaching consequences in individual cases, as the starting points that the law provides, in the abstract, for the calculation of sanction amount apply to both small and larger enterprises. In order to apply an administrative sanction (fine) that is effective, proportionate and with preventive character in all cases, the Commissioner's Office must adjust the amount of sanctions within the available range, but without exceeding the relevant legal ceiling. This may lead to a significant increase or decrease in the amount of sanction, depending on the circumstances of the case.

53. The Commissioner's Office considers it important to establish a fair distinction regarding the size of Controllers/Processors, when determining the starting point for calculating the amount of sanction indicated below and therefore takes into account its turnover[11]. However, this does not exempt the Commissioner's Office from the responsibility to carry out an examination of the effectiveness, proportionality and preventive character after calculating the amount of sanction[12] . The latter includes all the circumstances of the case, such as the commission of multiple infringements, the increase or decrease of the amount of sanction according to aggravating and mitigating circumstances, as well as financial/socio-economic circumstances. However, the Commissioner's Office should ensure that the same circumstances are not listed (considered) twice. In particular, the Commissioner's Office should not repeat the increase or decrease of the amount of sanction according to the company's turnover, but review its assessment of the appropriate starting value of the calculation.

54. For the reasons indicated above, the Commissioner's Office may consider adjusting the starting value of the calculation according to the degree of importance of the infringement, in cases where this violation is committed by an enterprise with an annual turnover of no more than 10,000,000 ALL, an annual turnover of no more than 50,000,000 ALL or an annual turnover of no more than 250,000,000 ALL[13]

[11]The Enterprise's Turnover is further discussed in Chapter 6.2 of this document.

[12] See Chapter 7.

[13] These values refer to the provisions of Law No. 43/2022, dated 21.04.2022 " *On the Development of Micro, Small and Medium-sized Enterprises* ", which provides for the categorization of enterprises, according to their turnover, into small, medium and large.

- For enterprises with an annual turnover ≤ 10,000,000 ALL, the Commissioner's Office may consider continuing to calculate the sanction amount based on an amount up to 0.2% of the identified starting point.

- For enterprises with an annual turnover of above 10,000,000 ALL up to 50,000,000 ALL, the Commissioner's Office may consider continuing to calculate the sanction amount based on an amount of up to 0.3% of the identified starting point.

- For enterprises with an annual turnover of over 50,000,000 ALL up to 250,000,000 ALL, the Commissioner's Office may consider continuing to calculate the amount of sanction based on an amount of up to 5% of the identified starting point.

55. For the same reasons, the Commissioner's Office may consider adjusting the starting value of the calculation according to the degree of importance of the infringement in cases where this infringement is committed by an enterprise with an annual turnover not exceeding 500,000,000 ALL, an annual turnover not exceeding 1,000,000,000 ALL or an annual turnover exceeding 1,000,000,000 ALL[14]

- For enterprises with an annual turnover of over 250,000,000 ALL up to 500,000,000 ALL, the Commissioner's Office may consider continuing to calculate the sanction amount based on an amount of up to 8% of the identified starting point.

- For enterprises with an annual turnover of over 500,000,000 ALL up to 1,000,000,000 ALL, the Commissioner's Office may consider continuing to calculate the sanction amount based on an amount of up to 15% of the identified starting point.

- For enterprises with an annual turnover above 1,000,000,000 ALL, the Commissioner's Office may consider continuing to calculate the sanction amount based on an amount of up to 40% of the identified starting point.

56. As a general rule, the higher the turnover of the undertaking within the applicable ceiling for it, the higher the calculation starting point is likely to be. This is particularly true for larger undertakings, for which the calculation starting point category has the widest range.

57. Furthermore, the Commissioner's Office is not obliged to apply this regulation to adjust the starting point of the calculation, if this does not appear necessary from the point of view of the effectiveness, proportionality and preventive character of the sanction.

58. It should be reiterated that these figures are a starting point for further calculations and not fixed amounts (price tags) for infringements of the provisions of the Personal Data Protection Law. The Commissioner's Office has the discretion to use the full range of sanction amounts, from the most minimal to the applicable legal ceiling, ensuring that the sanction amount is adapted to the circumstances of the case.

[14]These figures are added to bridge the gap between the highest threshold of the previous paragraph and the annual turnover threshold identified in Article 94, paragraphs 1, 2 and 3 of the Data Protection Law.

Example 6a – Identifying the starting point for further calculation of the sanction amount

A supermarket chain with a turnover of 2 000 000 000 ALL has infringed article 12 of the Personal Data Protection Law. The Commissioner's Office, based on a careful analysis of the circumstances of the case, decided that the infringement is of a low degree of importance. In order to determine the starting point for the further calculation of the sanction amount, the Commissioner's Office, first of all, notes that article 12 of the Personal Data Protection Law is listed in article 94, paragraph 2, letter "b" of the Law and that, based on the turnover of the Enterprise (2 000 000 000 ALL), a legal ceiling equal to 2 000 000 000 ALL is applied.

Based on the level of importance of the infringement, determined by the Commissioner's Office (low), the starting point of the calculation should range between 0 and 10% of the applicable legal ceiling [15](i.e. from 0 to 200,000,000 ALL). Based on the turnover of the undertaking (2,000,000,000 ALL), the Commissioner's Office may consider further reducing this amount to 40% of the identified starting point value, which corresponds to the level of importance of the infringement.

In the present case, the Commissioner's Office considered that – due to the relatively low level of importance of the infringement, compared to the relatively large turnover of the Enterprise – a starting point value of 40 000 000 ALL (which refers to a starting point value calculated at 100 000 000 ALL) is considered effective, proportionate and with preventive character. This amount constitutes the basis for the further calculation, which should result in a final amount that does not exceed the legal ceiling applicable to this case, equal to 2 000 000 000 ALL.

Example 6b – Identifying the starting point for further calculation of the sanction amount

A start-up application, with a turnover of 5 000 000 ALL, was found to have sold sensitive personal data of its customers to several data brokers for analytical purposes and, in this way, has infringed articles 6(1) and 9 of the Data Protection Law. The Commissioner's Office, based on a careful analysis of the circumstances of the case, has decided that the infringement is of a high degree of importance. In order to determine the starting point for the further calculation, the Commissioner's Office notes that articles 6 and 9 of the Data

[15]See paragraph 49, above.

Protection law are listed in article 94(2)(a) thereof and that, based on the turnover of the Enterprise (5 000 000 ALL), a statutory ceiling equal to 2 000 000 000 ALL applies [16].

Based on the degree of importance of the infringement determined by the Commissioner's Office (high), the starting point of the calculation should vary between 20 and 100% of the applicable legal ceiling (i.e. between 400,000,000 and 2,000,000,000 ALL of ceiling [17]). Based on the turnover of the Enterprise (5 000 000 ALL), the Commissioner's Office may consider further reducing this amount to 0.2% of the identified starting point value.

In the present case, (referring to a starting point value calculated at 400,000,000 ALL) the Commissioner's Office considers that a starting point value of 800,000 ALL is considered effective, proportionate and of a preventive nature. This amount constitutes the basis for the further calculation, which should result in a final amount that does not exceed the legal ceiling applicable to this case, equal to 2,000,000,000 ALL.

CHAPTER 5 – AGGRAVATING AND MITIGATING CIRCUMSTANCES

5.1 - Identification of aggravating and mitigating factors

59. Following the structure of the Personal Data Protection Law, after having assessed the nature, significance and duration of the infringement as well as its deliberate (intentional) or unintentional character, as well as the categories of personal data affected, the Commissioner's Office must take into account other aggravating or mitigating factors provided for in article 93, paragraph 2, letter "gj" of the Law.

60. For the assessment of these elements, the increase or decrease of the amount of a sanction cannot be predetermined through tables or percentages. It is worth reiterating that the level of the sanction will depend on all the elements collected during the administrative investigation and on further considerations related to previous experiences of the application of administrative sanctions (fines) by the Commissioner's Office.

61. For clarity, it should be noted that each criterion of article 93, paragraph 2 of the Personal Data Protection Law (regardless of whether assessed under Chapter 4 or this Chapter) - should be considered only once as part of the overall assessment of this article.

5.2 - Controller/processor actions in mitigating the harm suffered by data subjects

62. A first step in determining whether aggravating or mitigating circumstances have occurred is to examine article 93, paragraph 2, letter "c" of the Personal Data Protection Law, which relates

[16] Because this value is higher than 4% of the controller's turnover, which corresponds to 200,000,000 ALL.

[17] Ibid

to "*any action that the controller or processor has taken to mitigate the damage suffered by data subjects"*.

63. Data controllers and processors are obliged to implement technical and organizational measures to ensure a level of security appropriate to the risk, to carry out data protection impact assessments and to mitigate the risks to the rights and freedoms of individuals resulting from the processing of personal data. However, in the event of an infringement, the controller or processor must do everything possible to minimize the consequences of the breach for the individual(s) concerned.

64. Taking appropriate measures to mitigate the harm suffered by data subjects may be considered a mitigating factor, thus reducing the amount of the sanction.

65. The measures taken should be assessed, in particular, with regard to the time element, i.e. the time at which they are implemented by the controller or processor and with regard to their effectiveness. In this sense, measures implemented spontaneously before the initiation of the administrative investigation by the Commissioner's Office are more likely to be considered as a mitigating factor than measures implemented after that moment (the initiation of the investigation).

5.3 - Degree of responsibility of the controller/processor

66. According to article 93, paragraph 2, letter "ç" of the Personal Data Protection Law, the degree of responsibility of the controller or processor will have to be assessed taking into account the measures implemented by them, in accordance with articles 22 and 28 of the Law. The question that the Commissioner's Office must then answer is to what extent the controller did what could be expected to do, given the nature, purposes or scope of the processing, seen in the light of the obligations imposed on them by the provisions of the Personal Data Law.

67. In particular, in relation to this criterion – the residual risk to the freedoms and rights of data subjects – the harm caused to data subjects and the harm that continues after the measures taken by the controller, as well as the degree of durability of the measures taken in accordance with articles 22 and 28 of the Personal Data Protection Law, must be assessed.

68. In this context, the Commissioner's Office may also consider whether the data in question are directly identifiable and/or available without technical and organizational protection. However, it should be borne in mind that the existence of such protection does not necessarily constitute a mitigating factor [18]. This depends on all the circumstances of the case.

69. In order to adequately assess the above elements, the Commissioner's Office shall take into account any documentation made available by the controller or processor, e.g. in the context of the exercise of their right of protection. In particular, such documentation may contain evidence of when measures were taken and how they were implemented, whether there were

[18]See paragraph 70, below.

interactions between the controller and the processor (if applicable), or whether there was contact with the data protection officer or with data subjects (if applicable).

70. Considering the increased level of responsibility under article 6 of the Data Protection Law, compared to article 5 of the previous law, the level of responsibility of the controller or processor may be considered an aggravating or irrelevant factor in the case. Only in exceptional circumstances, where the controller or processor has gone above and beyond the obligations imposed on it, will this be considered a mitigating factor.

5.4 - Previous infringements of the controller/processor

71. Based on article 93, paragraph 2, letter "d" of the Data Protection Law, any previous infringement committed by the controller or processor must be taken into account when deciding whether to impose a sanction and when determining its measure.

5.4.1 - Time frame

72. First, attention should be paid to the moment when the previous infringement occurred, considering that the longer the time between a previous violation and the violation under administrative investigation, the lower its importance. Consequently, the more distant the time of the committed infringement, the less importance is given to it.

73. However, since infringements committed a long time ago may still be of interest when assessing the "processing activity records" of the controller or processor, no fixed limitation periods should be set for this purpose.

74. For the same reason, it should be emphasized that infringement of the Personal Data Protection Law, given that it is the new law in force, should be considered more important than violations of the provisions of the previous law, repealed with the entry into force of the current law.

5.4.2 – The case

75. For the purposes of article 93, paragraph 2, letter "d" of the Data Protection Law, previous data infringements of an entity, the same or different from the one being investigated, may be considered as "relevant".

76. Although all previous infringements may be an indicator regarding the general attitude of the controller or processor towards compliance with the provisions of the Personal Data Protection Law, more importance should be given to infringements of the same subject matter, as they are similar to the infringement found during the administrative investigation, especially when the controller or processor has previously committed the same infringement (repeated infringements). Thus, the same infringement of the subject matter under investigation should be considered more important than previous infringements related to a different subject matter.

77. For example, the fact that the controller or processor has failed in the past to respond, in a timely manner, to data subjects in the exercise of their rights, should be considered more relevant when the infringement under administrative investigation is also related to the controller's lack of reaction/response to a data subject in the exercise of his rights, than when it refers (merely) to a personal data breach.

78. However, previous infringements of a different case, but committed in the same way, should also be taken into account, as they may be indicative of ongoing problems within the controller's or processor's organization. This would be the case, for example, for infringements arising from the failure to follow the advice/recommendations of the relevant data protection officer.

5.4.3 - Other considerations

79. If an infringement committed during the time when the previous data protection law was in force is being considered, the Commissioner's Office takes into account the fact that the requirements/provisions of that law may differ from those of the current Personal Data Protection Law.

80. When considering the significance of a previous infringement, the Commissioner's Office must take into account the status of the proceedings in which the previous infringement was found – in particular any measures taken by the Commissioner's Office or by the court – in accordance with the previous law.

81. The existence of previous infringement may be considered as an aggravating factor in calculating the amount of the sanction. The weight given to this factor should be determined taking into account the nature and frequency of the previous infringements. However, the absence of any previous infringement cannot be considered a mitigating factor, since compliance with the provisions of the Personal Data Protection Law constitutes an explicit norm. If there is no previous infringement, this factor may be considered to have no impact.

5.5 - Degree of cooperation with the Commissioner's Office to remedy the infringement and mitigate its negative effects

82. Article 93, paragraph 2, letter “dh” of the Personal Data Protection Law requires the Commissioner's Office to take into account the degree of cooperation of the controller or processor, in order to correct the relevant infringement is rectified and its possible negative effects are mitigated.

83. Before further assessing the degree of cooperation of the controller or processor with the Commissioner’s Office, it should be noted that there is a general obligation for controllers/processors to cooperate with the Commissioner’s Office, expressly provided for in

article 84 of the Personal Data Protection Law, and that lack of cooperation may lead to the application of the sanction provided for in article 94, paragraph 3 of the Law. It should therefore be borne in mind that cooperation with the Commissioner's Office constitutes a common obligation for the controller/processor and, therefore, should be considered as a non-influential factor (and not as a mitigating factor) in the calculation of the sanction.

84. However, where cooperation with the Commissioner's Office has had the effect of limiting or avoiding negative consequences for the rights of individuals, the Commissioner's Office may consider this as a mitigating factor within the meaning of article 93, paragraph 2, letter "dh" of the Personal Data Protection Law, thus reducing the amount of the sanction. This may be the case, for example, where a controller or processor has responded in a particular manner to the requests of the Commissioner's Office during the administrative investigation phase, which has subsequently resulted in a significant limitation of the negative impact on the rights of individuals.

5.6 – The way the infringement was notified to the Commissioner's Office

85. Based on article 93, paragraph 2, letter "ë" of the Personal Data Protection Law, the manner in which the Commissioner's Office was notified of the infringement may constitute an aggravating or mitigating factor for the calculation of the sanction. In assessing this issue, particular weight may be given to the question of whether, how and to what extent, the controller or processor notified the Commissioner's Office of the infringement on his/its own initiative, before the infringement became known to the Commissioner's Office in other ways (e.g., through a complaint by the data subject, or an administrative investigation initiated *ex officio*). This circumstance is not relevant where the controller is subject to a specific notification obligation (such as, for example, in the case of personal data breaches under article 29 of the Personal Data Protection Law[19]. In these cases, the notification should be considered a non-influential factor.

86. When the infringement is brought to the attention of the Commissioner's Office, e.g., by a complaint or during an administrative investigation itself, this element should also, as a rule, be considered as a non-influential factor. The Commissioner's Office may consider as a mitigating circumstance the case where the controller or the processor has notified the infringement on its own initiative, before the Commissioner's Office becomes aware of the case.

5.7 – Compliance with previously assigned tasks on the same case

87. Article 93, paragraph 2, letter "f" of the Personal Data Protection Law provides that "*the implementation of corrective measures, where prior to the infringement these measures were given to the controller or processor in relation to the same matter*" must be taken into account

[19]It should be noted that a data *breach* does not always imply an infringement of the provisions of the Data Protection Law.

in assessing whether an administrative sanction of a fine will be imposed on the controller/processor, as well as in determining its amount.

88. Contrary to article 93, paragraph 2, letter "d" of the Personal Data Protection Law, this assessment refers only to the rectifying tasks that the Commissioner's Office itself has previously assigned to the same controller or processor in relation to the same matter.

89. In this context, the controller or processor may have a reasonable expectation that compliance with the duties previously imposed on it could prevent the occurrence/repetition of an infringement of the same nature in the future. However, since the fulfillment of the duties previously imposed by the Commissioner's Office is mandatory for the controller or processor, this element should not be taken into account as a mitigating factor in itself. On the contrary, an increased commitment on the part of the controller or processor in fulfilling the duties imposed (e.g., taking additional measures, beyond those ordered by the Commissioner's Office) is required, in order for this element to be considered as a mitigating factor in the calculation of the sanction amount.

90. On the contrary, failure to comply with a corrective measure previously ordered by the Commissioner's Office may be considered either as an aggravating factor or as a different/new infringement in itself, based on article 94, paragraph 3 of the Personal Data Protection Law. Therefore, it should be borne in mind that the same conduct cannot lead to a situation where it is administratively sanctioned (with a fine) twice.

5.8 – Compliance with approved codes of conduct and/or certification mechanisms

91. Article 93, paragraph 2, letter "g" of the Personal Data Protection Law emphasizes that compliance with codes of conduct, in accordance with article 35, or approved certification mechanisms, in accordance with article 37 of the Personal Data Protection Law, may be an important factor in assessing whether an administrative sanction of a fine will be imposed on the controller/processor, as well as in determining its amount.

92. Compliance with codes of conduct, or approved certification mechanisms in accordance with articles 35 and 37 of the Personal Data Protection Law, respectively, may constitute a mitigating factor in calculating the amount of the sanction. [20].

93. On the other hand, if the non-compliance with the codes of conduct, or certification, is directly related to the infringement found, the Commissioner's Office may consider this as an aggravating circumstance in calculating the amount of the sanction.

[20]This is also the position of the EDPB, expressed, among other things, in the guidelines of Working Group 235 (*WP253*).

5.9 - Other aggravating and mitigating circumstances

94. Article 93, paragraph 2, letter "gj" of the Personal Data Protection Law gives the Commissioner's Office a discretionary space to take into account any other aggravating or mitigating factors applicable to the circumstances of the case. In an individual case there may be many elements involved (which cannot all be listed exhaustively), which must be taken into account in order to ensure that the amount of sanction imposed is effective, proportionate and with a preventive character, in each case.

95. Article 93, paragraph 2, letter "gj", of the Personal Data Protection Law, mentions examples of aggravating or mitigating circumstances related to the circumstances of the case, such as financial benefits or losses avoided, directly or indirectly from the infringement. This provision is of fundamental importance for the adaptation of the sanction amount in the specific case. In this sense, this provision should be interpreted as an example of the principle of fair and just treatment of the relevant case.

96. The scope of this provision, which is necessarily non-exhaustive, should include all reasonable circumstances relating to the socio-economic context in which the controller or processor operates, as well as those relating to the legal context and those relating to the market context.

97. In particular, economic benefit from the infringement may be an aggravating circumstance, if the case results in the controller/processor deriving a benefit as a result of the infringement of the Personal Data Protection Law.

98. Circumstances that may lead to significant changes in the socio-economic context (e.g. the onset of a serious pandemic emergency, which may fundamentally change the way personal data are processed), may also be taken into consideration based on article 93, paragraph 2, the letter "gj", of Personal Data Protection Law.

The examples in this chapter are illustrations of the effect that aggravating and mitigating circumstances may have on the calculation of the amount of sanction. The increases or decreases mentioned in these hypothetical cases cannot be considered as precedents or indicators of the percentages that will be used in reality.

Example 7a – Assessment of aggravating and mitigating circumstances

A sports club used cameras equipped with facial recognition technology at the entrance to one of its locations, in order to identify the respective customers upon entry. Since the sports club carried out this processing in violation of article 9 of the Personal Data Protection Law (processing of biometric data, without a valid legal criterion), the Commissioner's Office, after investigating the violation, decided to apply an administrative sanction in fine. Taking into account all the relevant circumstances of the case, the Commissioner's Office considered this to be an infringement of a high degree of importance and, since the sports club had an annual turnover equal to 700 000 000 ALL, the starting point of the calculation

should vary between 20 and 100% of the applicable legal ceiling (i.e., between 400 000 000 ALL and 2 000 000 000 ALL). Based on the Controller's turnover (700,000,000 ALL), the Commissioner's Office considered further reducing this amount to 15% of the identified starting point value [21].

However, since the same sports club had been fined two years earlier for using fingerprint processing technology at the entrance to another of its locations, the Commissioner's Office decided to consider this as a repeated infringement (article 93(2)(d) of the Personal Data Protection Law). In doing so, the Commissioner's Office took into account the fact that this concerned almost the same subject matter and the infringement had been committed only two years earlier. Due to this aggravating factor, the Commissioner's Office decided to increase the amount of the sanction, for this specific case, to 124 800 000 ALL[22], not exceeding the applicable legal ceiling of 2 000 000 000 ALL.

Example 7b – Assessment of aggravating and mitigating circumstances

The operator of a car rental platform suffered a data breach, causing the personal data of its customers to be exposed to breaches for a short time. Taking into account all the relevant circumstances of the case, the Commissioner's Office assessed the operator's shortcomings in taking technical and organizational measures to guarantee the security of its platform as a violation of article 28 of the Personal Data Protection Law, as a violation of a low degree of importance. For this reason, the Commissioner's Office set as the starting point for calculating the sanction a value between 0 and 10% of the legal ceiling provided for in paragraph 1 (a) of article 94 of the Personal Data Protection Law (i.e., 0 to 100 000 000 ALL). Based on the Controller's turnover (1 100 000 000 ALL), the Commissioner's Office could consider further reducing this amount to 40% of the identified starting point value [23]. As above, the Commissioner's Office assessed as appropriate the application of a starting point for the further calculation of the sanction in the amount equal to 32 000 000 ALL.

The compromised personal data included copies of driving licenses and electronic ID cards. For this reason, all customers affected by the data breach were forced to re-apply for these documents, in order to limit the possibility of future identity theft. When informing data subjects about this incident, the operator offered all data subjects assistance in re-applying

[21] Assessing the circumstances of the case, the starting point for the further calculation of the sanction was taken as a value of 800,000,000 ALL.

[22] This illustrates the fact that the starting points for calculating the sanction amount do not limit the ability of the Commissioner's Office to take into account aggravating and mitigating circumstances in imposing a higher or lower sanction than the categories in question. As highlighted in Chapter 4, these figures constitute a starting point for further calculation of the sanction amount and not fixed values (price tags) for violations of the provisions of the law. The Commissioner's Office has discretion to use the full range of sanctions, from one ALL up to the legal ceiling, ensuring that the sanction amount is adapted to the circumstances of the case.

[23] By assessing the circumstances of the case (the turnover of the enterprise and the importance of the infringement), the starting value for the further calculation of the sanction was taken as 80,000,000 ALL.

for these documents with public institutions and set up a system for the reimbursement of any application fees paid. The Commissioner's Office considered this as an action to mitigate the damage suffered by data subjects (article 93(2)(c) of the Personal Data Protection Law), which had a mitigating effect on the sanction. Given the proactive stance and effectiveness of the measures taken by the operator, the Commissioner's Office decided to reduce the sanction to 16,000,000 ALL (again not exceeding the legal ceiling of 1,000,000,000 ALL).[24]

Example 7c – Assessment of aggravating and mitigating circumstances

A small credit rating agency was found to have infringed several provisions protecting the rights of data subjects, most notably by charging its clients a fee for exercising their right of access. The agency did this for all access requests. Taking into account all the circumstances of the case, the Commissioner's Office assessed that the infringements found were of a high degree of importance. For this reason, the Commissioner's Office set as the starting point for calculating the sanction a value between 20% and 100% of the legal ceiling provided for in paragraph 2 (b) of article 94 of the Personal Data Protection Law (i.e. 400 000 000 to 2 000 000 000 ALL). Since the agency had an annual turnover of 30,000,000 ALL, the Office considered it appropriate to apply a starting point for the further calculation of the amount of sanction equal to 2,400,000 ALL (given the size of the Controller, the starting point for the calculation of the sanction is reduced to 0.3% of the above starting point value).[25]

However, the Commissioner's Office took into account the fact that the agency had been able to benefit financially from the infringement, which constituted an aggravating circumstance (article 93(2)(gj) of the Personal Data Protection Law). With the aim of offsetting the benefits from the infringement, while maintaining an effective, proportionate and with preventive character impact of the sanction measure in this case, the Commissioner's Office decided to increase the amount of sanction to 30 000 000 ALL, not exceeding the legal ceiling of 2 000 000 000 ALL.

Example 7d – Assessment of aggravating and mitigating circumstances

A commercial company was found to have infringed the provisions of the Personal Data Protection Law, in particular due to the sale of its database for commercial advertising to its partners, which contained personal data regarding citizens who had not given their consent for this purpose.

[24] From the value of 32,000,000 ALL (resulting from the adjustment of 40% of the identified starting value of 80,000,000 ALL), a value of 50% has been removed, assessing proactive behavior to mitigate the damage. This example is for illustrative purposes only and does not imply that the Commissioner's approach will be such in every case. The Commissioner's Office may also assess a reduction of 2, 4 or even 5% of the value of 32,000,000 ALL.

[25] The starting point for adjusting the sanction depending on the turnover of the enterprise was a minimum value of 800,000,000 ALL, which was further adjusted to 0.3% according to the forecast for turnover.

Taking into account all the relevant circumstances of the case, the Commissioner's Office considered the violations found to be of medium importance and set as a starting point for calculating the amount of the sanction a value between 10% and 20% of the legal ceiling provided for in paragraph 2 (a) of article 94 of the Personal Data Protection Law (i.e., 200,000,000 to 400,000,000 ALL).
Since the company in question had an annual turnover of 40,000,000 ALL, it was deemed appropriate to reduce the starting point of the calculation to a value of 0.3% of the range of the starting point above. For this reason, it was deemed appropriate to apply a starting point for the further calculation of the sanction equal to 900,000 ALL.[26]

's Office further considered that this was a breach from which the controller had benefited, because the fact of not obtaining citizens' consent for the transmission of their data to the company's partners for the purpose of sending relevant advertisements had increased the amount of data that the controller could subsequently resell. Therefore, the Commissioner's Office considered the fact that the controller was able to benefit from the breach as an aggravating circumstance (Article 93 (2)(gj) of the Data Protection Act). Personal).

In order to counterbalance the benefits of the infringement, while maintaining an effective, proportionate and deterrent impact of the sanction, the Commissioner's Office decided to increase the amount of the sanction to 1,200,000 ALL, not exceeding the applicable legal ceiling of 2,000,000,000 ALL.

CHAPTER 6 – LEGAL CEILING AND CORPORATE RESPONSIBILITY

6.1 - Determination of the legal ceiling

99. The Personal Data Protection Law does not provide for fixed sanctions for specific violations. Instead, the law provides for general legal ceilings.

100. The sanction amounts measures provided for in the Personal Data Protection Law are legal ceilings, which do not allow the imposition of sanctions in excess of these values. In order to determine the exact legal ceiling, article 94, paragraph 3 of the Personal Data Protection Law should be taken into account, where applicable[27] . Therefore, the Commissioner's Office is obliged to ensure that these legal ceilings are not exceeded when calculating the amount of sanctions based on this methodology. Depending on the individual case, different legal ceilings may apply.

[26]The starting point for adjusting the sanction depending on the turnover of the enterprise was a minimum value of 300,000,000 ALL, which was further adjusted to 0.3% according to the forecast for turnover.
[27] See Subchapter 3.1.2.

6.1.1 – Static legal ceilings

101. Article 94 of the Data Protection Law provides for static ceilings and distinguishes between violations of different categories of obligations of the provisions of the law. As explained above in this document, paragraph 1 of article 94, establishes a legal ceiling of up to 1 000 000 000 ALL for violations of the obligations described therein, while paragraph 2 and 3 of the same article establish sanctions of up to 2 000 000 000 ALL for violations of the obligations described therein.

6.1.2 – Dynamic legal ceilings

102. In the case of an undertaking[28], the range of sanctions may be shifted towards a higher legal ceiling based on annual turnover [29]. This legal ceiling based on the undertaking's turnover is dynamic and individualized for a given undertaking (controller/processor), in accordance with the principles of effectiveness, proportionality and the preventive character of the amount of sanction.

103. More specifically, article 94, paragraph 1 of the Personal Data Protection Law allows for a legal ceiling of up to 2% of the annual global turnover, while paragraph 2 and 3 of this article provide for a legal ceiling of up to 4% of the annual global turnover (in both cases the global turnover reference is that of the previous financial year of the undertaking). The legal provisions require consideration of the static legal ceiling or the dynamic legal ceiling based on the annual global turnover of the undertaking and order the application of the highest value between them ("*whichever is higher*"). Consequently, legal ceilings based on annual turnover are applicable only if they exceed the static ceiling in a given case. This is the case when the annual global turnover of the undertaking for the previous financial year is more than 50 000 000 000 ALL. [30].

Example 8a – Dynamic legal ceiling

A credit reporting agency (CRA) collects and sells all creditworthiness data of all Albanian citizens to marketing and retail companies, without any legal basis for this. The agency's global annual turnover last year amounted to 80,000,000,000 ALL. In this case, the agency infringement, among other things, article 7 of the Personal Data Protection Law, a violation punishable by a sanction based on paragraph 2 of article 94 of the law. The static legal ceiling would amount to 2,000,000,000 ALL. The dynamic legal ceiling would amount to 3,200,000,000 ALL (4% of the turnover of 80,000,000 ALL). The sanction amount can reach up to 3,200,000,000 ALL, as this dynamic legal ceiling is higher than the static legal ceiling of 2,000,000,000 ALL. Consequently, the sanction is allowed to exceed the static

[28]See Subchapter 6.2.1 of this Methodology regarding the term *"enterprise"* .

[29]See Subchapter 6.2.2 of this Methodology regarding the term *"turnover"* .

[30]In the case of an annual turnover equal to 50,000,000,000 ALL, the maximum static legal ceiling (2,000,000,000 ALL) of Article 94 of the Law is equal to the dynamic legal ceiling (4% of global turnover) of this Article.

legal ceiling of 2,000,000,000 ALL, but it should not exceed the dynamic legal ceiling of 3,200,000,000 ALL.

Example 8b – Static legal ceiling

A sunglasses retailer operates an online store that allows customers to place their orders online. Through the order form, the retailer also processes personal data, including bank account details. The retailer does not provide adequate encryption of online transmission (https), making it possible for third parties to potentially intercept personal data during the transaction. The retailer violates article 28 (1) of the Personal Data Protection Law and may be subject to sanctions based on paragraph 1 of article 94 of the Law. The retailer's global annual turnover for the previous year amounts to 40 000 000 000 ALL. In this case, the static legal ceiling of 1,000,000,000 ALL is higher than the dynamic legal ceiling of 800,000,000 ALL (=2% of the turnover of 40,000,000,000 ALL), so the static legal ceiling prevails. Therefore, the amount of sanction, in this case, should not exceed the legal ceiling of 1,000,000,000 ALL.

Example 8c – Controllers and processors that are not undertakings

A municipality has an online system that allows its citizens to register for services, such as passport applications or marriage ceremonies. The municipality is the sole controller of this online system. Unfortunately, it has been found that the system also permanently transmits the data collected to external servers of a processor located in a country without an adequate level of data protection, where they are stored. In this case, no appropriate technical and organizational measures have been taken in relation to the transfer to the country in question. In addition to the transfer, the data are collected and processed on the basis of valid consent. The municipality has infringed article 41 of the Personal Data Protection Law, by transferring special categories of personal data to a third country without an adequate level of personal data protection, without the necessary guarantees/a lawful criterion for this purpose. Therefore, the municipality in question may be sanctioned in accordance with article 94, paragraph 2 of the Data Protection Law. Since the municipality is not included in the definition of an undertaking, the static legal ceiling is applicable in this case and, consequently, the amount of sanction should not exceed the value of 2 000 000 000 ALL.

6.2 - Determination of enterprise turnover and corporate responsibility

104. In order to determine the exact turnover for the dynamic legal ceiling, it is important to understand the concepts of "undertaking" and "turnover" as articulated in article 94 of the Personal Data Protection Law.

6.2.1 - Definition of an enterprise and corporate responsibility

105. Based on EU case law, the term "*undertaking*" includes any entity engaged in an economic activity, regardless of the legal status of that entity and the way in which it is financed [31]. Consequently, "undertakings" are identified as economic entities, rather than legal entities (subjects with separate legal personality). Different companies belonging to the same group of companies may form an economic entity and, consequently, an undertaking.

106. Consequently, the term "*undertaking"* may refer to a single economic entity (SEE), even if that economic entity is composed of several natural or legal persons. The formation of an SEE by several entities depends, in particular, on whether the SEE is free in its decision-making capacity or whether a leading economic entity, namely the parent company, exercises decisive influence over the others. The criteria for determining this influence are based on the economic, legal and organizational links between the parent company and its controlled one(e.g. degree of participation, personnel or organizational links, guidance and the existence of company contracts) [32].

107. In accordance with the doctrine of the SEE, article 94 of the Personal Data Protection Law follows the principle of direct corporate liability, which means that all actions committed or neglected by natural persons authorized to act on behalf of the undertaking are attributed to the latter and are considered as an act and infringement committed directly by the undertaking itself. The fact that some employees do not respect a code of conduct is not sufficient to avoid this attribution of liability. On the contrary, liability is excluded only when the natural person acts for his own private/personal purposes or for the purposes of a third party, thus becoming itself into a special controller (i.e. the natural person has acted beyond the powers granted to him).

108. Where a parent company owns 100% or almost 100% of the shares/capital of a controlled company, it will be presumed that the parent company is in a position to exercise decisive influence over the conduct of the controlled company. This applies even if the parent company does not own the total shares/capital directly, but indirectly through one or more controlled companies. In these circumstances, it is sufficient for the Commissioner's Office to prove that the controlled company is directly or indirectly, wholly or almost wholly owned by the parent company in order to conclude that the parent company exercises decisive influence.

109. However, the assumption set out above is not absolute, but can be rebutted by other evidence. To rebut the presumption in question, the company must provide evidence regarding the organizational, economic and legal links between the subsidiary and the parent company, which are adequate to demonstrate that they do not constitute a SEE, regardless of whether the parent company owns 100% or almost 100% of the capital of the controlled company. In

[31] See EU case law; Case C-41/90, *Höfner and Elser v Macrotron GmbH* , paragraph 21; Joined Cases *C* -159 and 160/91, *Poucet and Pistre v Assurances Générales de France* , paragraph 17; Case 364/92, *SAT Fluggesellschaft mbH v Eurocontrol* , paragraph 18; Joined Cases *C* -180-184/98, *Pavlov and Others* , paragraph 74; Case C-138/11, *Compass-Datenbank GmbH v Republic of Austria* , paragraph 35.

[32] Case C-90/09 P, *General Química and Others v Commission.*

determining whether a controlled company acts autonomously, account must be taken of all relevant factors relating to the links between the controlled company and the parent company, which may vary from case to case and, therefore, cannot be set out in an exhaustive list.

110. If, on the other hand, the parent company does not own all or almost all of the capital of the controlled company, additional facts must be established to justify the existence of a SEE. In this case, it is necessary to demonstrate not only that the parent company has the ability to exercise decisive influence over the subsidiary, but also that it has actually exercised such decisive influence, so that it can interfere at any time with the subsidiary's freedom of choice and determine its conduct.

111. The sanction is addressed to the (co-)controller/processor and the Commissioner's Office has the option to consider the parent company jointly and severally liable for the payment of the sanction.

6.2.2 - Determination of turnover

112. Turnover is derived from the annual financial statements of an undertaking (specifically from the “profit and loss” statement), which provide an overview of the previous financial year of a company or a group of companies (consolidated financial statements). Turnover within the meaning of article 94 of the Data Protection Law should be understood as net turnover, which means the value derived from the sale of goods/services, after deduction of value added tax (VAT) and other taxes directly related to turnover. This turnover does not include income from sporadic transactions, which are not related to the scope of the undertaking’s activity.

113. If the undertaking is subject to the obligation to prepare consolidated financial statements, these consolidated financial statements of the parent company, which heads the group, are relevant for reflecting the combined (global) turnover of the undertaking. If such statements do not exist, any other document that is appropriate for ascertaining the annual global turnover of the undertaking for the relevant financial year shall be obtained and used.

CHAPTER 7 – EFFECTIVENESS, PROPORTIONALITY AND PREVENTVE CHARACTER

114. The sanction imposed for infringements of the Personal Data Protection Law must be effective, proportionate and with a preventive nature in each individual case. In other words, the sanction amount imposed must be adapted to the infringement committed in its specific context.

115. As explained in Chapter 4, the assessment carried out in this chapter covers the entirety of the sanction imposed and all the circumstances of the case, including e.g. the accumulation of multiple infringements, increases and decreases according to aggravating and mitigating circumstances, and financial/socio-economic circumstances.

7.1 - Effectiveness

116. In general, a sanction can be considered effective if it achieves the objectives for which it was imposed (be it to restore compliance with the rules, to punish illegal behavior, or both).

117. As set out in article 93, paragraph 2 of the Personal Data Protection Law, the Commissioner's Office must assess the effectiveness of the sanction in each individual case. For this purpose, due regard must be paid to the circumstances of the case and, in particular, to the assessment made above, bearing in mind that the sanction must also be proportionate and preventive, as described below.

7.2 - Proportionality

118. The principle of proportionality requires that the measures taken do not exceed what is appropriate and necessary to achieve the objectives legitimately pursued by data protection legislation. Where there is a choice between several appropriate measures, the least onerous must be considered and the disadvantages caused must not be disproportionate to the aims pursued.

119. It follows that the sanctions must not be disproportionate to the objectives pursued (i.e. compliance with the rules relating to the protection of data of natural persons), and that the amount of sanction must be proportionate to the infringement, taking into account, in particular, the degree of its importance.

120. Therefore, it is necessary to verify that the amount of sanction is proportionate to the severity of the infringement and the size of the enterprise to which the entity that committed the violation belongs, and that the sanction imposed in this way should not exceed what is necessary/necessary to achieve the objectives pursued by the provisions of the Personal Data Protection Law.

121. As a specific derivative of the principle of proportionality, the Commissioner's Office may consider further reducing the amount of the sanction on the basis of the controller/processor's inability to pay. Any such reduction requires exceptional circumstances. Thus, there must be objective evidence that the imposition of the sanction would irreversibly jeopardize the economic viability of the undertaking in question. Furthermore, the risks must be analyzed in a specific social and economic context.

    a) **Economic viability**: The undertaking must submit detailed financial data (for the last five years, as well as projections for the current year and the next two years) in order for the Commissioner's Office to examine the likely future development of key factors such as solvency, liquidity and profitability. The mere circumstance that an undertaking is in a bad financial situation, or will be after a large amount of sanction, does not satisfy the requirement in question, since the recognition of such an obligation would be tantamount

to granting an unjustified competitive advantage to undertakings less adapted to market conditions [33].

b) **Proof of loss of value**: The amount of sanction may only be deducted if its imposition would endanger the economic viability of the undertaking and would cause its assets/assets to lose all or most of their value. A direct causal link must be shown between the sanction and the significant loss in value of the assets/assets. Furthermore, it cannot be disputed that the amount of sanction has threatened the economic viability of an undertaking when the latter had decided on its own to liquidate its activity and sell all its assets/assets. The undertaking must prove that it is likely to exit the market and its assets/assets will be broken up or sold at significantly lower prices, with no alternative for the undertaking (or its assets/assets) to continue operating on the market.

c) **Specific social and economic context**: Specific economic context may be considered if the sector in question is going through a cyclical crisis (e.g., suffering from *overcapacity* or falling prices) or if enterprises have difficulties accessing capital or credit, as a result of prevailing economic conditions. Specific social context is likely to be present in the context of high unemployment at regional or wider level.

122. If the criteria are met, the Commissioner's Office may take into account the inability of the enterprise to pay the sanction and reduce its amount accordingly.

7.3 – Preventive character

123. Finally, a sanction with a preventive character is one that has a real deterrent effect. In this respect, a distinction can be made between general deterrence (discouraging others from committing the same offence in the future) and specific deterrence (discouraging the offender from committing the same offence again).

124. A sanction is of a preventive nature when it restrains an individual from infringing the objectives pursued, as well as the rules established, by the provisions of the law. Decisive, in this context, is not only the nature and extent of the sanction, but also the possibility of its imposition. Anyone who commits a violation must understand that the sanction will indeed be imposed on him.

CHAPTER 8 – FLEXIBILITY AND REGULAR EVALUATION

125. The above chapters reflect a general methodology for calculating sanction amounts. However, this general methodology should not be misunderstood as a form of automatic, or arithmetic, calculation of the sanction amount. Individual determination of the sanction must always be based on a humane assessment of all the relevant circumstances of the case and must be effective, proportionate and preventive character in relation to that specific case.

[33] See EU case law, inter alia, in joined cases *C* -189/02 P, C-202/02 P, C-205/02 P to C-208/02 P and C-213/02 P, *Dansk Rørindustri and Others v Commission.*

126. It should be noted that this methodology cannot anticipate every possible feature of a infringement and therefore cannot be exhaustive. Consequently, this methodology is subject to regular review to assess whether its implementation effectively meets the objectives required by the Personal Data Protection Law. The Commissioner's Office may revise this methodology based on its further experiences in the daily practical application of the law as well as on the practice followed by the EU supervisory authorities and, in particular, the BEMD. The Commissioner's Office may repeal, amend, restrict or replace this methodology at any given time, with effect for the future.