

COMMENTS ON PUBLIC CONSULTATION VERSION OF GUIDELINES 04/2022 ON THE CALCULATION OF ADMINISTRATIVE FINES UNDER THE GDPR

Foreword

The provisions referred to in Art. 83 GDPR, aimed at establishing administrative pecuniary sanctions applicable for violations of the provisions of the Regulation, present a relevant number of criticalities at the interpretative level, due to their formulation with specific regard to the choice of identifying only the maximum limit of the amounts sanctions by defining two thresholds applicable for a double groups of heterogeneous kinds of violations.

In some national contexts (such as the Italian one), the national legislation as reformed for adaptation to the GDPR have provided for the application of the aforementioned maximum limits of the pecuniary sanctions referred to in Art. 83 also with regard to the violation of further provisions in force only at national level.

On the basis of the well-known case law that emerged at European level, on the basis of which the administrative pecuniary sanctions imposed by the independent administrative authorities have been traced back to "criminal matters"¹, the application of these sanctions must be supported by specific guarantees to be identified in compliance with principles of legality and certainty-determinacy of the offenses sanctioned. These principles are also reaffirmed in various national legislation which have adopted specific rules on pecuniary administrative sanctions².

On the contrary, the aforementioned setting of art. 83 with regard to administrative pecuniary sanctions, given the exclusion of an implementing regulation, gives the national supervisory authorities an excessive margin of discretion in determining and grading sanctions in specific cases, even if in compliance with the aforementioned principles of effectiveness, proportionality and dissuasiveness, and with the general criteria indicated in Art. 83.2, GDPR.

The current wording of art. 83 makes it impossible to estimate beforehand and difficult to verify subsequently the sanction imposed against a specific violation by a data controller, and entails unjustifiable differences in treatment with respect to similar situations examined by various national supervisory authorities (as is already happening), also jeopardizing one of the main objectives of the GDPR, that is to standardize the protection of the data subjects and the obligations and responsibilities of the data controllers and processors. This setting could cause a progressive increase in disputes and burdening of the activities of the supervisory authorities themselves, where it is not possible to establish clear, unambiguous and coherent criteria in advance, as set out in the guidelines document in consultation.

Based on these general considerations, with the present document, we intend to formulate below some comments with specific regard to Chapter 6 - LEGAL MAXIMUM AND CORPORATE LIABILITY and, in particular, to paragraph 6.2 - "Determining the undertaking's turnover and corporate liability", for the purpose of examining the doubts that may arise from the current indications provided on the determination of turnover to be taken into consideration for the purpose of calculating the sanction in the case of undertaking and group of the undertaking and on the possible joint and several liability envisaged for the parent companies (paragraphs 118 to 127).

¹ See, among others, the judgments of the European Court of Human Rights in the Grande Stevens v. Italy, appeal n. 18640/10, and of the Court of Justice of the European Union 26 February 2013, case C-617/10, Åklagaren v. Hans Åkerberg Fransson.

² See, for example, Italian law no. 689/1981 which, in the initial articles (articles 1-12) recalls the principles of legality, personality and certainty.

Undertaking and Group of undertakings

1. In summary, in par. 6.2.1, points 118 to 126, of the guidelines under consultation, there is an interpretative reconstruction of the concept of "undertaking" indicated in art. 83, paragraphs 4, 5 and 6, GDPR, which starting from recital 150, in reference to art. 101 and 102 TFEU, goes as far as to recall the case law of the CJEU on competition law to envisage the notion of "undertaking" as a single economic unit (SEU), postulating that where there is 100% or almost 100% control of an undertaking over another, there is the presumption that the parent company has a decisive influence on the choices of the subsidiary, with the consequence of the possibility of considering the combined turnover of the companies that make up the SEU as a reference point for determining the maximum dynamic limit of the sanction to be inflicted (2 or 4% of the annual global turnover if greater than, respectively, 10 or 20 million euros).

In focusing instrumentally for the notion of undertaking on the reference to recital 150, paragraphs 118 and 119 of the guidelines however provide a partial and not fully correct representation of the framework of the recitals and provisions of the GDPR, within which (in the official version in English language) there are actually various terms in order to indicate different aspects and forms of business activity ("enterprise", "group of undertakings", "corporate", "group of enterprises", "undertaking"), used with meanings different in the following provisions.

However, there is a formal element that most of all cannot escape the interpreter and that is not sufficiently valued for the purposes that concern us, namely the fact that in any case the GDPR explicitly provides for a formal definition of group of undertakings in the Art. 4.19, to be understood precisely as *"a controlling undertaking and its controlled undertakings"*.

This concept is also better clarified in recital 37 GDPR:

"A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings." [ed: underscore by the writer].

It should be noted that this recital is not even mentioned in the reconstruction made in paragraphs 118 and following of the guidelines, while the same concept is then taken up again in recital 48, in which reference is made to: *"Controllers that are part of a group of undertakings ... may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected."*

The concept of group of undertakings is also taken up in the definition of "binding corporate rules" pursuant to art. 4.20 GDPR, which refers to *"personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity;"*.

The omission of any reference to the aforementioned recital 37 appears rather anomalous in several respects, given that, as can be read, the definition of "group of undertakings" is not only completely equivalent to the concept of SEU obtainable from the aforementioned jurisprudence of the CJEU on the subject of competition law, but above all it is more specific in relation to the matter of data protection, referring to a control on the processing of personal data and not to an economic control.

Therefore, in a systematic perspective, also taking into account the criteria followed in the technique of drafting the regulatory texts, if the European legislator had considered that the administrative pecuniary sanctions could also be determined on the basis of the global annual turnover of a group of undertakings, it would have had to refer to the relevant definition contained in Art. 4.19 GDPR (which, as mentioned, corresponds to that obtainable indirectly from the exegetical reconstructions referred to in the well-known judgments of the CJEU on competition matters).

In light of the aforementioned principles of legality-certainty-determinacy, the literal formulation of the provision, in which reference is made to "an undertaking" and not to a "group of undertaking", therefore entails an insuperable formal limitation, which would make voidable any administrative sanction pecuniary payment based not on the turnover of the company that committed the violation, but on that of the parent company and / or the business group to which it belongs, understood in the terms set out above.

It is also highlighted the further difficulty deriving from the fact that, in the official Italian version of the GDPR, the same term "impresa" is always used for the English concepts of "enterprise", "undertaking" and "corporate". Therefore, from a national perspective, further problems could arise in terms of interpretation for the national data protection authority and for the judicial authorities called upon to examine the amount of the sanction in the event of its appeal by the addressee, given that art. 83, par. 4 and 6, refers only to an undertaking and not to a group of undertaking or enterprises and that it would be necessary to refer to the definition of "impresa" pursuant to art. 4.18 of the GDPR and not to that of the group of undertakings referred to in art. 4.19.

In this sense, we ask the Board to take into account the observations formulated above and review the paragraphs indicated, integrating them with an in-depth analysis of the definition of group of undertakings, as defined in recital 37, and clarifying the relationship between this definition and the concept of SEU derived from the CJEU jurisprudence, with respect to the provision "in case of an undertaking" pursuant to art. 83, paragraphs 4,5 and 6, GDPR.

2. In any case, even if it was considered possible to overcome the objections formulated above regarding the definition of group of undertakings (4.19) as obtainable from the related recital 37, it is evident how the reconstruction of the concept of undertaking as a single economic unit formulated by the CJEU jurisprudence in reference to the application of art. 101 and 102 TFEU (referred to in recital 150), must necessarily be integrated with one or more elements relating to data protection laws and the overall structure of the GDPR regarding the imputation of obligations and responsibilities in this matter, essentially based on the combined disposed of accountability and risk-based approach.

In this sense, it should be excluded the possibility of quantifying a sanction against a company only by virtue of an economic control by another company, which does not also translate into a control, by the parent company, over the data processing activities of the said company.

In fact, it is believed that the rules on obligations and related violations present in the GDPR, in line with the relative overall structure, are subjectively focused on a concept of legal unit (data controller or processor also operating within a group of undertakings or of enterprises) and are not to be interpreted, as envisaged in the guidelines in consultation, recalling the concept of an undertaking as a single economic unit.

Possibly more legal units (undertakings) can be considered as recipients of a sanctioning provision where, as mentioned, there is a control (or in any case a sharing of decisions) on the activities, purposes and means of processing, for which also the determination of the quantum of the sanction should follow this approach.

Moreover, if reference were made exclusively to the concept of economic unit, one would be faced with a substantial problem: the recognition of the possibility of identifying the maximum limit of sanctions by taking

as a reference the worldwide turnover not of the single company/data controller (and of any branches or factories), but of the business group to which it belongs would create a strong misalignment with the underlying structure of the GDPR.

So, for a specific data processing, the national data protection authorities should first identify the data controller and then, in the eventual determining sanction phase, abstract from the concept of controller and responsibility, identify any parent company or group to which the data controller belongs and, where present, use the group turnover as the basis for calculating the maximum limit of the sanction, by virtue of a simple presumption of an economic nature (so-called Azko presumption) which, in the opinion of the writer, would not be justifiable in the context of data protection, which should always be based on the verification of the decisive influence or control exercised by the parent company, by virtue of the economic, organizational and legal ties, on the processing of personal data carried out by the controlled undertaking, as expressly provided for by the aforementioned recital 37 .

There would therefore be the risk of effectively configuring a sort of "strict liability" on an economic level for each parent company for the violations committed by the subsidiaries in terms of data protection, which is completely unacceptable and not provided for by the relevant laws, which would also entail a reversal of the burden of proof, as the supervisory authority can limit itself to verifying that 100% or almost 100% of the shareholding in the capital of the infringing company is held, even indirectly, by a parent company and should be then the companies have to demonstrate that they are not constituting a SEU (a proof that, in many ways, we could define as "diabolica", if we adhere only to criteria of an economic nature, in case of ownership of 100% of the share capital).

The economic criterion envisaged in the paragraphs under examination (118-126) of the guidelines under consultation should at least be supplemented by a criterion of a legal nature, such as that reported in recital 37 (".. An undertaking which controls the processing of personal data in undertakings affiliated ... "), also in consideration of the totally different areas governed by the regulations in question (respectively the right to competition and the right to data protection), aimed at recalling the indispensability for the supervisory authorities not to proceed only on the basis of a simple presumption, but to verify whether the parent company, by virtue of the economic, organizational and legal aspects of the relations in place with the subsidiary responsible for the violation, exercises a decisive influence or control over the personal data processing activities, a necessary and unailing element to in order to parameterize the sanction on the turnover at group level.

In this direction, it is recommended to proceed with a revision of paragraphs 120, 121 and 122 and from 124 to 125, with integration or reference to the concept of control on data processing expressed for group of undertakings in the context of recital 37, and to eliminate or reformulate the generic and unjustified indication referred to in point 127 on the right for the supervisory authority to provide for joint and several liability of the parent company in the payment of the sanction by the subsidiary, even if it is a legally autonomous subject, on the basis of the aforementioned presumption of purely economic control and not also a control on the personal data processing.

3. The SEU criterion suggested in par. 6.2.1 of the guidelines under consultation is to be reviewed and integrated also in relation to other factors, including, first of all, that represented by the heterogeneity of the economic activities carried out by companies belonging to group of undertakings, governed by different sectoral laws under the supervision of separate supervisory or regulatory authorities.

These heterogeneous structures in the composition of the group of undertakings or business groups clearly have significant impacts also in terms of the obligations and responsibilities relating to the processing of personal data and can lead to strict regimes of separation of the activities and of the segregation of

information between the companies belonging to the same. group (think of the so-called financial conglomerates and groups formed by companies operating in various sectors such as, for example, banking, finance, insurance, telecommunications, tertiary, distribution and services, etc.).

Also from this point of view the proposed criterion (the purely economic one) would be inadequate and unreasonable, if not accompanied also by an evaluation focused on some sharing, involvement or control of the parent company (often only holding companies) or of other companies of the group in the economic activity from which the processing of personal data of the company author of the violation derives, in order to be able to possibly take into account the turnover of the parent company or group for the purpose of determining the dynamic legal maximum.

Instead, the possibility of resorting to the simple presumption of the decisive influence of the parent company at 100% or almost, should be excluded a priori, where there is no homogeneity of economic activities and processing of personal data with respect to the controlled company.

In this sense, if the sanction is to be determined on the basis of the group turnover, a more reasonable criterion should be to consider, possibly, the turnover generated by the specific economic activity from which the processing of personal data derives, certainly not the overall turnover generated by distinct and autonomous economic activities carried out in other areas or sectors.

Secondly, the suggested criterion does not seem to take sufficient account of the aspects deriving from any corporate changes, such as mergers and incorporations.

In fact, it often happens that, from the moment in which a proceeding is initiated against a company to the moment in which a sanction is imposed, a few years can pass (the proceedings can be very long: in Italy, for example, up to 5 years, term within which the right to obtain payment of the sanction is prescribed, pursuant to art.28 of law 689/1981). During this period, control of a company may have passed from one parent company to another.

As is known, the law provides that, where the dynamic criterion for determining the maximum limit is taken into account, reference is made to the previous year with respect to the sanction. The fact that the sanction can arrive after several years therefore implies, if the criterion suggested by the guidelines under consultation is applied, the concrete possibility that for the purpose of determining the sanction itself, is taken into account the turnover of a different group that of which the company was a party at the time of the violation, even going so far as to attribute joint and several liability to the new parent company.

Therefore, if the criterion indicated were to be maintained, a discrimination should at least be introduced aimed at not involving a group other than that of which the company was part at the time of the violation

Failing that, it would also be enormously difficult to manage corporate mergers and acquisitions, since clauses and indemnities would have to be inserted to regulate this eventuality.

Finally, we invite you to reflect and provide clarifications also on the repercussions that the criterion proposed in the guidelines in consultation could have in relation to the management of relations between companies (controllers) and their suppliers (processors).

In fact, where a company must take into account, as a sanction risk, also what could derive from a calculation based on the group of undertakings to which it belongs, and therefore should be considered potentially recipient of enormous sanctions, the guarantees and indemnities to be requested from suppliers should be equally high.

In fact, it would be difficult to determine a priori the legal and sanctioning risks that the company may have to manage, with repercussions on the entire production chain.