Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 12 (61) No. 2 – 2019
https://doi.org/10.31926/but.scl.2019.61.12.2.26

SOME CORRELATIONS BETWEEN THE PRINCIPLES RELATING TO PERSONAL DATA PROCESSING AND THE RECORDS OF PROCESSING ACTIVITIES

Silviu-Dorin ȘCHIOPU[1]

Abstract: *In this short paper we intend to examine how the records of processing activities can facilitate the operator's obligation to demonstrate compliance with the principles relating to the processing of personal data and we will argue that the record of processing activities is an instrument that can support the analysis of the implications of any processing and the controller should keep extended records of processing activities in order to also demonstrate at least in part the compliance with the principles set out in article 5 of the General Data Protection Regulation (GDPR).*

Key words: *GDPR, personal data, principles relating to processing, records of processing activities, compliance, accountability.*

1. The accountability principle

Recital (74) of the General Data Protection Regulation (GDPR) provides that "the controller should […] be able to demonstrate the *compliance* of processing activities with this Regulation […]". On this line, usually any processing should comply with the principles relating to the processing of personal data set out in article 5 GDPR and the controller should be able to demonstrate such compliance under the principle of accountability. Furthermore, according to article 85 paragraph (5) letter a) GDPR, the infringement of the basic principles for processing may result in administrative fines up to 20.000.000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In order to demonstrate compliance with the GDPR, recital (82) states that the controller "should maintain *records of processing activities* under its responsibility" and article 30 paragraph (4) GDPR provides that the controller will make the record available to the supervisory authority on request. Thus, under the principle of accountability, the controllers are required to actively demonstrate compliance and not merely wait for data subjects or supervisory authorities to point out the shortcomings (European Union Agency for Fundamental Rights, Council of Europe, 2018, p. 138).

The proper identification of all data processing operations and the maintenance of an

[1] *Transilvania* University of Braşov, silviu-dorin.schiopu@unitbv.ro

inventory of data processing operations as an accountability measure is not a novel idea (Article 29 Working Party, 2010, p. 11), but only since the 25th of May, according to article 30 paragraph (5) GDPR, it became mandatory for most controllers (Article 29 Working Party, 2018b, p. 2) to keep records of the processing activities carried out under their responsibility. Also, article 83 paragraph (4) letter a) GDPR provides that the infringement of the controller's obligation to maintain a record of processing activities and/or make the record available to the supervisory authority is sanctioned just as the infringement of the basic principles for processing.

In view of the above, in the following we will study to what extent the records of the processing activities can demonstrate not the compliance with the GDPR in general, but with the principles relating to the processing of personal data set out in article 5 GDPR in particular, principles that we need to keep in mind every time we interpret the rules of the GDPR (Șandru, 2018b. p. 364).

2. The principle of lawfulness

Article 5 paragraph (1) letter a) GDPR requires personal data to be processed *lawfully* in relation to the data subject. The principle of lawfulness implies the need for a legitimate ground, such as the consent of the data subject, the performance of a contract, the performance of a task carried out in the exercise of public authority, the compliance with a legal obligation, the legitimate interests of the controller or third parties, or the protection of the data subject's vital interests.

The mandatory entries in the record of processing activities referred to in article 30 paragraph (1) GDPR do not include the specification of the processing's legal basis. Thus, if the controller chooses to include only the mandatory minimum information, the record will not prove the compliance of the processing activities with the principle of lawfulness.

However, nothing prevents the operator from including in the record of processing activities any other information in addition to those expressly provided in the article 30 (1) GDPR. Therefore, for an overview of the lawfulness of all personal data processing activities, the operator should include the legal basis of the processing in the record of processing activities, all the more so since the supervisory authorities of some Member States (for example Belgium, United Kingdom and Luxemburg) included in their published models the mention of the legal basis of the processing.

3. The principle of fairness

Article 5 paragraph (1) letter a) GDPR requires personal data to be processed *fairly* in relation to the data subject. With regard to fair and transparent processing recital (60) states that the data subject should be informed of the existence of the processing operation and its purposes and the controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. According to the 2018 Handbook on European data protection law, the principle of fairness governs primarily the relationship between the controller and the

data subject, "goes beyond transparency obligations and could also be linked to processing personal data in an ethical manner" (European Union Agency for Fundamental Rights, Council of Europe, 2018, p. 118-119).

Furthermore, recital (39) states that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data". Therefore, under the principle of fairness, "the data subject must be informed of the risk to ensure that processing does not have unforeseeable negative effects" (European Union Agency for Fundamental Rights, Council of Europe, 2018, p. 117) and should not be taken by surprise at a later point about the ways in which their personal data has been used (Article 29 Working Party, 2018a, p. 1).

The obligation to process data fairly also implies that information as to the processing is provided to the data subject in a timely manner and data controllers have to consider the reasonable expectations of data subjects, the effect that the processing may have on them and their ability to exercise their rights in relation to that processing. That's why, the position of Article 29 Data Protection Working Party was that, "wherever possible, data controllers should, in accordance with the principle of fairness, provide the information to data subjects well in advance of the stipulated time limit" (Article 29 Working Party, 2018a, p. 16). Not the least, in accordance with this principle, the information provided should be as meaningful as possible.

Although the principle of equity is difficult to define and therefore it is difficult to assess the effects of its application in the practice of personal data controllers (Șandru, 2018a, p. 63), the multiple facets of the principle of fair processing should not lead to the conclusion that the record of processing activities cannot be used to prove the conformity of the processing with this principle. However, the content of the records will need to be corroborated with other documented elements, including that, should the legitimate interests of the data subject so require, "the controller is prepared to go beyond the mandatory legal minimum requirements of service to the data subject" (European Union Agency for Fundamental Rights, Council of Europe, 2018, p. 75).

4. The principle of transparency

Article 5 paragraph (1) letter a) GDPR requires personal data to be processed in a *transparent* manner in relation to the data subject. Under the GDPR transparency is considered intrinsically linked to fairness and the principle of accountability (Article 29 Working Party, 2018a, p. 5).

According to recital (39), "it should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed". Transparency also refers to the information provided to data subjects following a request of access to their own data. So, under this principle, the controller must provide to the data subjects information related to the fair processing of their personal data. Furthermore, recital (58) states that "the principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used".

From the minimum content of the record of processing activities provided by the article 30 paragraph (1) GDPR it does not appear if the processing complies or not with the principle of transparency. In order to demonstrate compliance with this principle, following the example offered by the Belgian supervisory authority and their model records of processing activities, controllers should include in their records information on how data subjects are informed about the processing of their data according to articles 12-14 GDPR.

5. The principle of purpose limitation

Article 5 paragraph (1) letter b) GDPR requires personal data to be collected for *specified*, *explicit* and *legitimate* purposes and not further processed in a manner that is incompatible with those purposes. Thus, the principle of purpose limitation requires that any processing of personal data must be done for a specific well-defined purpose and only for additional, specified, purposes that are compatible with the original one (Article 29 Working Party, 2013). However, further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with article 89 paragraph (1) GDPR, is not be considered to be incompatible with the initial purposes.

The specification of the purpose influences other requirements, including the adequacy, relevance and proportionality of the data collected (data minimisation principle), their accuracy (data accuracy principle) and the requirements regarding the period of data retention (storage limitation principle). Since the controller, according to article 30 paragraph (1) letter b) GDPR, must indicate in the records of processing activities the purposes of the processing, it should be fairly easy to also check whether the declared purpose complies with the requirements of the principle of purpose limitation.

6. The data minimisation principle

Article 5 paragraph (1) letter c) GDPR requires personal data to be *adequate*, *relevant* and *limited* to what is necessary in relation to the purposes for which they are processed. Also, recital (39) states that "personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means".

In order to verify that the processing complies with the data minimisation principle, the controller should check if the purpose of the processing cannot be fulfilled by other means and then, if the answer is negative, correlate the categories of personal data that the records of processing activities must contain according to article 30 paragraph (1) letter b) GDPR with the purpose of the processing.

7. The data accuracy principle

Article 5 paragraph (1) letter d) GDPR requires personal data to be *accurate* and, where necessary, *kept up to date*. Also, every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are

processed, are erased or rectified without delay. Just as the data minimisation principle, the data accuracy principle must also be seen in the context of the processing's purpose. For example, if the purpose of storing data is principally to document the chronology of events, such records must not be changed.

On the other hand, controllers such as the Romanian Credit Bureau, which provides information regarding individuals who have outstanding loans with banks or financial companies, must make special efforts to comply with the principle of accuracy considering that the data subjects may suffer negative effects if the data provided is incorrect or outdated.

Therefore, the purpose of the processing will determine the extent to which personal data should be updated. In order to keep track of the compliance with the data accuracy principle, the record of processing activities should include the date of the last update of the information relating to each data processing included in the register and whether or not that data needs to be updated.

8. The storage limitation principle

Article 5 paragraph (1) letter e) GDPR requires personal data to be kept in a form which permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

Just as the data minimisation principle and the data accuracy principle, the storage limitation principle must also be seen in the context of the processing's purpose. Thus, personal data must be deleted or anonymised when they are no longer needed for the purposes for which they were collected.

However, personal data may be stored for longer periods insofar as the personal data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89 paragraph (1) GDPR subject to implementation of appropriate technical and organisational measures in order to safeguard the rights and freedoms of the data subject.

Regarding the records of processing activities, according to article 30 paragraph (1) letter f) GDPR, where possible, the controller must indicate the envisaged time limits for erasure of the different categories of data. "It is not sufficient for the data controller to generically state that personal data will be kept as long as necessary for the legitimate purposes of the processing. Where relevant, the different storage periods should be stipulated for different categories of personal data and/or different processing purposes, including where appropriate, archiving periods" (Article 29 Working Party, 2018a, p. 38-39). Therefore, the controller could use the entries in the registry to demonstrate the compliance of processing activities with the storage limitation principle.

9. The data security principle

Article 5 paragraph (1) letter f) GDPR requires personal data to be processed in a manner that ensures appropriate security of the personal data, including protection

against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. These measures should take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. Also, according to article 30 paragraph (1) letter g) GDPR, where possible, a general description of these technical and organisational security measures must be included in the records of processing activities.

In view of the above, by respecting the requirement of maintaining the record of processing activities, the controller will also be able to demonstrate compliance with the principle of integrity and confidentiality.

10. Conclusions

This brief overview of the correlation between the principles relating to processing of personal data and the content of the record of processing activities shows that controllers should have an interest in keeping a more extended record than that provided for in article 30 paragraph (1) in view of the fact that, at least in part, it will demonstrate as well the compliance with the principles laid down in article 5 of Regulation (EU) 2016/679, insofar as the entries in the register have also been implemented in practice.

References

Article 29 Working Party (2010). *Opinion 3/2010 on the principle of accountability*, WP173, adopted on 13 July 2010. Retrieved from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf.

Article 29 Working Party (2013). *Opinion 03/2013 on purpose limitation*, WP203, adopted on 2 April 2013. Retrieved from http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Article 29 Working Party (2018a). *Guidelines on transparency under Regulation 2016/679*, WP260 rev.01, as last Revised and Adopted on 11 April 2018. Retrieved from http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025.

Article 29 Working Party (2018b). *Position paper on the derogations from the obligation to maintain records of processing activities pursuant to Article 30(5) GDPR*. Retrieved from http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51422.

European Union Agency for Fundamental Rights, Council of Europe (2018). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

Șandru, D.-M. (2018a). Principiul echității în prelucrarea datelor cu caracter personal [The fairness principle in personal data processing]. *Pandectele române, 3*, 57-63.

Șandru, D.-M. (2018b). Principiile protecției datelor – de la teorie la practică [Principles of data protection – from theory to practice]. *Curierul judiciar, 6*, 364-366.