Law Review • vol. XI, issue 1, January-June 2021, pp. 83-88

An Example of Exercising the Right of Access Against a Romanian Civil Court Acting in Its Judicial Capacity

Silviu-Dorin Şchiopu*

Abstract

The right to access one's own data is explicitly acknowledged as a fundamental right in Article 8 (2) of the Charter of Fundamental Rights of the EU which states that "Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified" and is regulated under Article 15 of the General Data Protection Regulation (GDPR). Although the Romanian courts and other judicial authorities must ensure compliance with the rules of the General Data Protection Regulation which regulates the right of access by the data subject, the data protection supervisory authorities are not competent to supervise processing operations of courts when acting in their judicial capacity and our national legislator did not entrust this mission to specific bodies within our judicial system. Consequently at least one court considered that the scope of Article 15 GDPR does not include its jurisdictional activity. Therefore, this study will present a practical case on the effective judicial remedy for the infringement by a civil court of the right to access. The main conclusion after analysing the effective remedy can only be that, despite the adage iura novit curia, it is necessary to raise awareness on data protection regulation even among those called to apply the law.

Keywords: *European Union Law, national law, personal data, data protection, civil courts, court proceedings, judicial activities, online disclosure, right to access, effective judicial remedy.*

Preliminary considerations

Article 8 (2) of the Charter of Fundamental Rights of the European Union[1] states that "(e)veryone has the *right of access* to data which has been collected

* https://orcid.org/0000-0002-9927-1016. E-mail: dorinxschiopu@gmail.com. All links were last accessed on 18 April 2021. A draft of this article was presented at the 7th *Annual International Conference on Law and Administrative Justice from an Interdisciplinary Perspective*, organized by the National University of Political Studies and Public Administration, Faculty of Public Administration, Department of Law "Victor Dan Zlătescu", Bucharest (Romania) on 26-28 November 2020 (https://administratie publica.eu/ro/node/128).

[1] Published in the Official Journal of the European Union C 326 from 26 October 2012.

concerning him or her" and this fundamental right is regulated under Article 15 of the General Data Protection Regulation (GDPR)[2].

Recital (63) of Regulation (EU) 2016/679 indicates the purpose of this right: "(a) data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and *verify, the lawfulness of the processing*". As such, the data subjects have the right to obtain from the controller confirmation as to whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data and the information mentioned in article 15 (1) (a) - (h) and article 15 (2) GDPR.

One piece of information that the controller should provide to the data subject, as a result of exercising the right of access, is the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period. This information is of interest in relation to the processing of litigants' personal data by making it available on the courts portal.

In this context we must remember the *storage limitation principle* provided for in Article 5 (1) (e) GDPR, principle according to which personal data shall be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed" and which must be correlated with the *right to erasure*, provided for in Article 17 (1) (a) GDPR, that can be invoked by the data subject when "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed"[3].

Thus, on the one hand we have the *obligation of the controller* to respect the principles related to the processing of personal data, as provided in Article 5 (2) GDPR, and on the other hand we have the *right of the data subject* to obtain from the controller the erasure of personal data when the latter are no longer necessary for the purposes for which they were collected or processed.

As mentioned in Recital (78), the controller should adopt internal policies and implement measures which meet in particular the principles of data protection *by design* and data protection *by default*. Consequently the controller has an obligation to implement appropriate technical and organisational measures,

---

[2] *Regulation (EU) 2016/679* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, published in the Official Journal of the European Union L 119 from 4 May 2016.

[3] As natural oblivion has become inoperative in the context of information technology, whereas any data posted online may remain accessible for an indefinite period and the Internet has transferred the "curse" of eternal remembrance onto its users, it was necessary to establish appropriate legal mechanisms to ensure that the spectre of the past will not forever haunt the data subjects. See, Andreea Verteş-Olteanu, *Art. 17 din Regulamentul general privind protecţia datelor – un prim pas în direcţia uitării dreptului de a fi uitat*, in Andrei Săvescu (ed.), RGPD – Regulamentul general privind protecţia datelor cu caracter personal. Comentarii şi explicaţii, Bucureşti: Hamangiu, 2018, p. 50.

such as *pseudonymisation*, which are designed to implement data protection principles, such as data minimisation, in an effective manner.

Article 4 (5) GDPR defines 'pseudonymisation' as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information". The processing of litigants' personal data by making it available on the courts portal is justified by the *purpose of the portal* during the settlement of the case and which is no longer required after the settlement, respectively the archiving of the file[4]. The purpose of the court portal is to ensure the transparency of court proceedings, by the possibility of any interested person to follow the evolution of cases before the court, by consulting the lists of court hearings, including court terms and solutions given in settled cases.

In the light of the legislation on personal data protection, in 2012 the Superior Council of Magistracy Plenary considered that it is necessary to develop a procedure to delete or censor personal data on the court portal in case of archived files, given that after archiving a file on the court portal, it can be further identified by the number and object of the case[5].

Nowadays, the courts portal mentions that "in principle at this moment, on the portal of the courts can be consulted only the files that are pending or have not left the courts ledger for more than 3 years"[6]. It is therefore unclear when the courts actually implement the principle of data minimization and the principle of storage limitation in relation to solved disputes, i.e. the moment when the name of the litigants (data subjects) is anonymized on the portal.

One of the ways in which a data subject can find out this information is by submitting a request of access under Article 5 GDPR and the court (the controller) should provide to the data subject the envisaged period for which the personal data will be displayed on the portal, or, if not possible, the criteria used to determine that period. Nothing simpler – in theory – since the right of access by the data subject is *expressis verbis* provided for in Article 15 GDPR.

The courts as personal data controllers in the General Data Protection Regulation

The courts are mentioned several times in the Regulation (EU) 2016/679. According to Article 37 (1) (a) on the designation of the data protection officer,

---

[4] *Press release of 17 May 2012* regarding the Decision of the Superior Council of Magistracy Plenary to notify the Ministry of Justice with the proposal to delete or censor personal data from the court portal in the case of archived files, available on https://www.juridice.ro/wp-content/uploads/2012/05/CSM-17-05-date-cu-caracter-personal.doc

[5] *Ibidem*.

[6] http://portal.just.ro/SitePages/termeni.aspx. For the past situation, see Adrian Cristolovean, *Aspects of Personal Data Processing by Romanian Civil Courts Acting in Their Judicial Capacity*, Law Review, special issue, 2019, p. 117-118.

the controller shall designate a person with expert knowledge of data protection law and practices to assist the controller to monitor internal compliance with the GDPR[7] in any case where the processing is carried out by a public authority or body, *except for courts acting in their judicial capacity*. Also, Article 55 (3) on the competence of the supervisory authority provides that the supervisory authorities *shall not be competent to supervise processing operations of courts acting in their judicial capacity*[8].

In view of the above, one might be led to believe that the General Data Protection Regulation does not apply to the processing of personal data by of courts acting in their judicial capacity. However, the provisions of Regulation (EU) 2016/679 must be interpreted in the light of the recitals in its preamble and Recital (20) indicates that "this Regulation applies, inter alia, to the activities of courts and other judicial authorities".

The recital further states that "the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making".

But the most interesting part of Recital (20) mentions that "(i)t should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations."

An access request and the correlative answer given by a court as a personal data controller

Late 2019, Braşov Tribunal as a personal data controller registered an access request formulated pursuant to Article 15 (1) and (3) of Regulation (EU) 2016/679. In the reply sent to the data subject, the Tribunal refused to grant the access request, stating that the provisions of Article 15 GDPR do not concern its jurisdictional activity (i.e. for example the parties), but only its own staff. Therefore, in the opinion of the Tribunal, the right of access must be interpreted as meaning that its scope encompasses only the court employees and consequently the courts are not be required to respond to access requests from other data subjects such as the litigants.

---

[7] Recital (97).

[8] For further details, see Hielke Hijmans, *Article 55 Competence*, în C. Kuner, L. A. Bygrave, C. Docksey (eds.), „The EU General Data Protection Regulation (GDPR). A Commentary", Oxford: Oxford University Press, 2020, p. 909-910.

Since the Romanian supervisory authority is not competent to supervise processing operations of courts acting in their judicial capacity and the Romanian legislation did not entrust the supervision of such data processing operations to specific bodies within the national judicial system, the data subjects may appeal only to the right to an effective judicial remedy against a controller provided by Article 79 GDPR[9] when a court refuses to provide the information mentioned in article 15 (1) (a) - (h), such as the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period.

Late 2020, in the application of the right to an effective judicial remedy, at the request of the data subject, Braşov Tribunal acting in its judicial capacity[10] found that the litigants enjoy the right of access under Article 15 GDPR[11] and forced Braşov Tribunal in its capacity as personal data controller to comply with the access request[12].

Conclusions

The two exceptions established for the benefit of the courts are of strict interpretation and application – *exceptio est strictissimae interpretationis* – so that the scope of the obligations and rights provided for in Article 15 GDPR regarding the data subjects cannot be narrowed in the absence of a restriction corresponding to the conditions provided by Article 23 of Regulation (EU) 2016/679. Also, personal data controllers, including the courts, should not lose sight of the fact that the provisions of the General Data Protection Regulation must be interpreted in the light of the correlative recitals.

In the absence of a specific body within the Romanian judicial system to supervise the data processing operations carried out by the courts, the compliance with the rules of Regulation (EU) 2016/679 falls onto the president of the court since, according to Article 43 (1) of the Law no. 304 of 28 June 28 2004

[9] According to Article 79 GDPR, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with Regulation (EU) 2016/679.

[10] Due to the rules of jurisdiction, the Tribunal was the competent court to resolve the claim of the data subject, although the defendant was the Tribunal itself, as a personal data operator.

[11] See Braşov Tribunal, second section of civil, administrative and fiscal litigation, *civil sentence no. 910/CA/2020*, ECLI:RO:TBBRV:2020:012.000910, available on http://rolii.ro/hotarari/60652a17e49009a42400003f.

[12] Since the judgment is not final and the Tribunal, acting as a personal data controller, has declared an appeal, we will return on another occasion to the storage of litigants' data on the court portal after the Court of Appeal has favourably resolved the appeal and the judgment will be enforced. Only then should we have a clear answer on the period for which the litigants' personal data remain available on the courts portal.

on judicial organization[13], each court is headed by a president who exercises managerial duties in order to organize its activity efficiently. But who is to enhance the awareness among the court presidents on their obligations under the General Data Protection Regulation in the absence of the specific body mentioned by Recital (20)?

[13] Republished in the Official Journal of Romania, Part I, no. 827 from 13th of September 2005.