Law Review ● special issue, Decembre 2019, pp. 113-122

ASPECTS OF PERSONAL DATA PROCESSING BY ROMANIAN CIVIL COURTS ACTING IN THEIR JUDICIAL CAPACITY*

*Adrian CRISTOLOVEAN***

Abstract: *Although the data protection supervisory authorities are not competent to supervise processing operations of courts when acting in their judicial capacity, the General Data Protection Regulation also applies to the activities of courts and other judicial authorities which must ensure compliance with the rules of this regulation. Therefore this paper aims to explore the processing performed by civil courts in their judicial capacity, without overlooking the impact of the internet age on the publication of personal data from pending cases and judgments. To this end we'll analyse the provisions of Regulation (EU) 2016/679 and the national legal framework regarding the processing of data by the courts, without overlooking a recent trend in dealing with processing operations performed by the Court of Justice of the European Union (CJEU). At first glance it seems that our civil courts were left to their own devices as to data protection since the Romanian national supervisory authority is not competent to supervise processing operations of courts acting in their judicial capacity and the Romanian legislator did not entrust this mission to specific bodies within our judicial system. However despite the absence of a right to lodge a complaint with a supervisory authority or to an effective judicial remedy against a supervisory authority, the data subjects – plaintiffs and defendants – may resort to the right to an effective judicial remedy against the controller for the protection of their personal data processed by a civil court. Since the right to the protection of personal data is not an absolute right and it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality, not always will prevail the rights of the data subject, or, better said, they will not be able to prevail before the balance tilts – sooner or later – in favour of the data subject.*

Key words: *Private Law, European Union Law, GDPR, civil courts, court proceedings, court decisions, judicial activities.*

Introduction

The General Data Protection Regulation (GDPR)[1] expressly refers to the activity of the civil courts[2] on several occasions. Firstly, recital (20) mentions that

* The article was prepared for the International Law Conference, "*Current Issues within EU and EU Member States: Converging and Diverging Legal Trends*", 3rd edition, organized by the Faculty of Law – Transilvania University of Braşov on the 29th-30th of November 2019. All links were last accessed on 4 November 2019.

** LL.M. Attorney at law (Bucharest Bar) – Muşat & Asociații (adrian.cristolovean@musat.ro).

while this Regulation applies, *inter alia*, to the activities of courts and other judicial authorities, the competence of the supervisory authorities[3] should not cover the processing of personal data when the courts are acting in their judicial capacity. Hence, in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making, civil courts don't fall under the control of ordinary supervisory authorities. However, Member States can entrust the supervision of such data processing operations to specific bodies within their judicial system, an aspect that the Romanian legislator did not consider at the time of implementing Regulation (EU) 2016/679[4].

Such specific bodies should, in particular: *a).* ensure compliance with the rules of this Regulation (*e.g.* the obligation to keep records of processing activities and to implement the principles of data protection by design and by default[5]), *b).* enhance awareness among members of the judiciary of their obligations under this Regulation, *c).* handle complaints in relation to such data processing operations.

The need to establish the aforesaid structures is substantiated by the fact that courts – when acting in their judicial capacity – are also exempted from the obligation to designate a data protection officer[6], namely a person with expert knowledge of data protection law and practices that should assist the civil courts to monitor internal compliance with the General Data Protection Regulation, including awareness-raising and training of staff involved in processing operations.

---

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

[2] Our analysis does not consider the processing of personal data by *criminal courts*, aspects covered by *Directive (EU) 2016/680* of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, published in the Official Journal of the European Union L 119 from 4 May 2016. This directive was transposed into national law by *Law no. 363 from 28 December 2018*, published in The Official Journal of Romania, Part I, no. 13 from 7 January 2019.

[3] *Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal* in Romania, established by Law no. 102 from 2 May 2005, published in The Official Journal of Romania, Part I, no. 391 from 9 May 2005.

[4] *Law no. 190 from 18th of July 2018* on implementing measures for 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 […], published in The Official Journal of Romania, Part I, no. 651 from 26th of July 2018, doesn't contain any provision in this regard, nor any other law.

[5] For further details see S.-D. Şchiopu, *The obligation to keep a record of processing activities for personal data*, Revista română de drept al afacerilor no. 1/2018, p. 85-94; S.-D. Şchiopu, *An Overview of the Technical and Organisational Measures Necessary to Ensure the Effective Implementation of the General Data Protection Regulation*, Revista română de drept al afacerilor no. 2/2019, p. 53-56.

[6] See recital (97) and article 37 (1) (a) GDPR.

At first glance, it seems that civil courts were left to their own devices as to data protection given the absence of an obligation to designate a data protection officer, the fact that the Romanian national supervisory authority is not competent to supervise processing operations of courts acting in their judicial capacity and our legislator did not entrust this mission to specific bodies within our judicial system. However we have to bear in mind that Regulation (EU) 2016/679 applies to the activities of courts and other judicial authorities, despite the abovementioned derogations, and civil courts must ensure compliance just as any other controller should[7].

1. Personal data processing in court proceedings

The Code of Civil Procedure[8] requires that the decision be delivered in public hearing[9] (article 402) and the court hearings are public, except for the cases provided by law (article 17). Conducting civil proceedings without public presence can happen according to article 213 (1) when the court, upon request or ex officio, orders that they be carried out in whole or in part without the presence of the public. This can happen when a public hearing would undermine morality, public order, the interests of minors, the privacy of the parties or the interests of justice.

In a jurisprudential interpretation "[t]he principle of publicity means that the civil proceedings are, as a rule, conducted before a court in a public hearing, in the presence of the parties, but also of any other person who wishes to attend the debate. Thus, the publicity takes place in court, not in virtual space, including the presence of the audience in the court room. This does not mean that people who do not want to attend the debates must subsequently be given access to information on the various litigations that were pending before the court"[10].

It is obvious and unavoidable that during the procedure before the civil court personal data will be processed usually by disclosure[11], especially those of the

---

[7] Article 4 (7) GDPR: "«controller» means the natural or legal person, public authority, agency or other body which, alone or jointly with others, *determines the purposes and means* of the processing of personal data; where the purposes and means of such processing are determined by […] law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law".

[8] *Law no. 134 from 1 July 2010* regarding the Code of Civil Procedure, republished in the Official Journal of Romania, Part I, no. 247 from 10 April 2015.

[9] According to article. 396 (2) from the Code of Civil Procedure, when the decision was postponed, it can also be delivered not in public hearing, but by making the solution available to the parties through the court clerk.

[10] Bucharest Court of Appeal, VIII[th] section for administrative and fiscal litigation, *civil ruling no. 10 from 19 March 2015*, and S.-D. Şchiopu, *Personal Data Processing. Retrieval of Information Available on the Courts' Portal. Right of Opposition of the Data Subject.* […] *Principle of Publicity of Court Hearings*, Revista română de jurisprudenţă no. 1/2018, p. 83 and 86.

[11] Article 4 (7) GDPR: "«processing» means any operation or set of operations […], such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval,

plaintiff and the defendant, as part of the normal course of the judicial proceedings, even maybe special (sensitive) categories of personal data[12] whose processing is in principle prohibited according to article 9 (1) GDPR, one exception being precisely the need for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity. For instance a person's name and surname are personal data, whether or not they are sufficient in a given situation to identify that person[13].

It is worth to mention that civil courts will not base the lawfulness of processing on the consent of the data subjects but on other legal grounds[14] provided by the General Data Protection Regulation such as the compliance with a legal obligation to which the controller is subject or the performance of a task carried out in the public interest, considering that justice is regarded as a public service[15].

However nowadays there is an exception to this rule. Some courts offer the possibility to request the communication of documents in electronic format and online access to the electronic court case file. As the party can truly choose the way procedural documents are communicated – by email or traditional mail services – and the court file can be consulted either online, either in physical format at the court archive, the processing necessary for the use of these electronic means will be based on the consent of the data subject according to article 6 (1) (a) GDPR. In this specific case consent should be regarded as freely given because the data subject has a genuine free choice since consent can be withdrawn without detriment, that is, without losing access to the documents related to the court proceedings.

The civil court will also be responsible for the conformity with the principles relating to processing of personal data pursuant to article 5 GDPR[16] and must be able to demonstrate, in accordance with the accountability principle, the compliance of processing activities with Regulation (EU) 2016/679.

---

consultation, *use, disclosure by transmission, dissemination or otherwise making available*, alignment or combination, restriction, erasure or destruction".

[12] *E.g.* data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, data concerning health or data concerning a natural person's sex life or sexual orientation.

[13] High Court of Cassation and Justice of Romania, the panel for questions of law, *decision no. 37 from 7 December 2015*, published in the Official Journal of Romania, Part I, no. 51 from 25 January 2016.

[14] D.-M. Şandru, *Situations in which the processing of personal data is allowed without the consent of the data subject*, in A. Săvescu (coord.), RGPD – Regulamentul general privind protecția datelor cu caracter personal: comentarii şi explicații, Bucharest: Hamangiu, 2018, p. 39-48.

[15] See article 5 of *Law no. 304 from 28 June 2004* on judicial organization, republished in the Official Journal of Romania, Part I, no. 827 from 13 September 2005.

[16] For further details see S.-D. Şchiopu, *The Pillars of Personal Data Processing*, Revista Universul Juridic no. 6/2017, p. 96-101; D.-M. Şandru, *Principles of Data Protection - from Theory to Practice*, Curierul judiciar no. 6/2018, p. 364-366.

2. The online publication of personal data from pending cases and judgments

The publication on the courts' portal (http://portal.just.ro/) of personal data from court files is done in accordance with the Strategy for Computerization of the Judicial System[17]. It concerned, inter alia, the transfer and publishing of *public data* about court cases, decisions and rulings from ECRIS (The Electronic Court Register Informational System) on the portal of the Ministry of Justice. This Government Decision is considered to have created for the civil courts the legal obligation to make available online on the courts' portal personal data such as the names of the plaintiffs and the defendants[18].

Although the implementation of the strategy should have been aimed at securing personal information, our national supervisory authority recommended to the Ministry of Justice only to take "measures for the exact determination of personal data that are strictly necessary to achieve the purpose pursued through the ECRIS application, respectively the courts' portal, provided the data must be adequate, relevant and not excessive [in relation to the purposes for which they are processed[19]] (posting only the name and surname of the defendants and plaintiffs in the published solution)"[20].

On the other hand, the Plenary of the Superior Council of Magistracy considered that "it is necessary to elaborate a procedure that allows the deletion or censorship of personal data from the portal of the courts in the case of archived court files" and decided notify the Ministry of Justice, in its capacity as administrator of the portal of the courts, with the indicated aspects[21].

This decision was based on the following facts: *a).* personal data should only be kept for the period of time necessary to fulfil the purpose for which they were collected or for further processing; *b).* the content of the right to the protection of personal data, which concerns the right of the natural person to the protection of

---

[17] Approved by *Government Decision no. 543 of 9 June 2005*, published in the Official Journal of Romania, Part I, no. 547 of 28 June 2005.

[18] See for instance Constanța Court of Appeal, section for administrative and fiscal litigation, *civil ruling no. 14 from 2 February 2015*, available on http://rolii.ro/.

[19] Recital (28) from *Directive 95/46/EC* of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, published in the Official Journal of the European Communities L 281 from 23rd of November 1995.

[20] S.-D. Şchiopu, *The effectiveness of the right to be forgotten*, in I. Alexe, N.-D. Ploeşteanu, D.-M. Şandru (eds.), Protecția datelor cu caracter personal. Impactul protecției datelor personale asupra mediului de afaceri. Evaluări ale experienţelor româneşti şi noile provocări ale Regulamentului (UE) 2016/679, Bucharest: Universitară, 2017, p. 191-192.

[21] *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.

the characteristics that lead to his identification and the correlative obligation of the state to take adequate measures to ensure an effective protection; *c).* the purpose of the court portal to ensure the transparency of the judicial procedures, through the possibility of any interested person to follow the evolution of the cases submitted to the court, by consulting the lists of sessions of the court, including the deadlines and the solutions given in court cases; *d).* data processing, by posting the name of the parties on the portal, which is justified by the purpose of the portal during the trial of the case and which, is no longer required after the case has been resolved, namely the archiving of the file; *e).* the fact that after archiving a file from the courts' portal, it can still be identified by the number and object of the case[22].

Since nothing happened in the meantime and the personal data continued to appear on the portal after the court case files were archived, the Judicial Inspection proposed not long ago the analysis by the Legislation and Documentation Service within The Superior Council of Magistracy of the possibility to delete information from courts' computer databases and identifying the solutions that may be available to them in the case of requests made by the parties regarding the removal of identification data from these records and from the court portal, given the two applications filed in 2016 at the High Court of Cassation and Justice[23]

As far as we know, until the archiving deadline is fulfilled, deadline established in relation to the subject matter of the case, the data provided by the ECRIS program continue to be in the electronic records of the files that are not confidential and implicitly also remain published on the court's website[24]. Consequently, at present the deletion of personal data from the portal does not take place at the time of archiving the court files, but at the completion of the archiving period.

As the Court of Justice of the European Union (CJEU) has also stated "even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive [requirements laid down in Article 6 (1) (c) to (e) of Directive 95/46, now repeated in Article 5 (1) (c) to (e) of Regulation 2016/679] where those data are no longer necessary in the light of the purposes for which they were collected or processed. That is so in particular where they appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed"[25].

---

[22] *Ibidem*.

[23] Superior Council of Magistracy, Judiciary Inspection, *Control report no. 1619/IJ/917/DIJ/2016*, 22 April 2016, http://old.csm1909.ro/csm/linkuri/19_07_2016__82228_ro.doc.

[24] Ploieşti Court of Appeal, section for administrative and fiscal litigation, *decision no. 91 from 10 February 2015*, available on http://rolii.ro/.

[25] CJEU, *Judgment from 13 May 2014*, C‑131/12, Google Spain, ECLI:EU:C:2014:317, published in the electronic Reports of Cases (Court Reports - general), paragraph 93. See also CJEU, *Judgment from 24 September 2019*, C‑136/17, GC and Others (Déréférencement de données sensibles), ECLI:EU:C:2019:773, published in the electronic Reports of Cases (Court Reports - general), paragraph 74, which reiterates this idea but also in the context of the General Data Protection Regulation.

The processing of personal data by keeping them on the portal after the dispute is settled clearly violates the principles of minimisation[26] and storage limitation set by article 5 (1) (c) and (e) GDPR, posting the name of the parties on the portal, which is justified by the purpose of the portal during the trial of the case, is no longer necessary after the case has been settled, namely the archiving of the physical court case file.

Therefore, pursuant article 17 (1) (a) GDPR, the data subjects should obtain from the civil courts the erasure of data concerning them from the portal, since the personal data are no longer necessary in relation to the purposes for which they were processed[27]. However, the civil courts could show a proactive attitude towards the compliance with Regulation (EU) 2016/679 and request the administrator of the portal to implement technical measures that will ensure *ex officio* the anonymisation of online data concurrently with the physical archiving of the file.

Unlike the national legal framework, the *Rules of Procedure of the Court of Justice*[28] provide for more specific regulations regarding the anonymisation of personal data. According to article 95 (1), in the proceedings pending before it, the Court respects the anonymity granted by the referring court or tribunal. Also, if it considers it necessary, the Court may also render anonymous data subjects concerned by the case[29]. In order to maintain its effectiveness, the Court recommends that the application be made at the outset of the proceedings, since, on account of the dissemination of information concerning the case on the Internet, granting anonymity becomes much more difficult if the notice of the case concerned has already been published in the Official Journal of the European Union[30].

Not long ago, the Court of Justice of the European Union decided to go even further and anonymise all requests for preliminary rulings involving natural

---

[26] As one author said, this principle "is very important in Romania, since most laws provide obligations for controllers that establish the legality of the processing, but clearly violate the data minimization" – D.-M. Şandru, *Old principles in new times. Critical remarks on two newly introduced phrases in Article 5 of General Data Protection Regulation*, Revista română de drept al afacerilor no. 1/2018, p. 83.

[27] Silviu-Dorin Şchiopu, *General considerations on the right to the erasure of personal data*, Revista Universul Juridic no. 9/2019, p. 48.

[28] CJEU, *Consolidated version of the Rules of Procedure of the Court of Justice* of 25 September 2012, as last amended on 9 April 2019, https://curia.europa.eu/jcms/upload/docs/application/pdf/2012-10/rp_en.pdf.

[29] At the request of the referring court or tribunal, at the duly reasoned request of a party to the main proceedings or of its own motion. When requested by a party, the application for anonymity must be made by a separate document stating appropriate reasons.

[30] CJEU, *Practice Rules for the Implementation of the Rules of Procedure of the General Court* adopted by the General Court on 20 May 2015, https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-08/dpe_vc_en.pdf.

persons[31]. This concern arose in the context of the application of Regulation (EU) 2016/679, at which point the Court decided to increase the protection of the data of natural persons in publications concerning requests for preliminary rulings. Practically the Court followed the tendency, seen within the member states[32], to increase the protection for personal data against a background marked by the proliferation of means of searching and disseminating information.

Consequently, in order to ensure the protection of the natural persons' data while guaranteeing at the same time that citizens are informed and have the right to open courts[33], the Court of Justice decided, in all requests for preliminary rulings brought after 1 July 2018, to replace, in all its *public documents*, the name of natural persons involved in the case by initials. Similarly, any additional element likely to permit identification of the persons concerned will be removed. In the case of decisions issued by the Romanian civil courts, before being published by the Foundation "Romanian Legal Information Institute" (http://rolii.ro/)[34] the name, surname, nickname, date and place of birth, personal numeric code, address and occupation of the data subjects are anonymised[35].

However, the Court of Justice of the European Union stressed that its measures seek to ensure appropriate protection for personal data only in the publications of the Court of Justice and these measures do not affect the way in which cases are handled by the Court or the usual progress of the proceedings, or, in particular, the hearings, which will continue to follow the current arrangements.

3. The right of the data subject to an effective judicial remedy against a civil court

Given that, according to article 55 (3) GDPR, common supervisory authorities aren't competent to supervise processing operations of civil courts acting in their judicial capacity, neither the plaintiff, nor the defendant from a civil litigation can lodge a complaint as data subjects with the Romanian supervisory authority. As a consequence, there is also no question of an effective judicial remedy against a

---

[31] CJEU, *Press release no. 96/18*: From 1 July 2018, requests for preliminary rulings involving natural persons will be anonymised, Luxembourg, 29 June 2018, https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-06/cp180096en.pdf.

[32] See also C. de Terwangne, *Diffusion de la jurisprudence via internet dans les pays de l'Union européenne et règles applicables aux données personnelles*, 2005, http://www.crid.be/pdf/public/5021.pdf.

[33] „Tout en garantissant l'information des citoyens et la publicité de la justice" – in the French version of the Press release no. 96/2018.

[34] S.-D. Şchiopu, *Online Published Civil Judicial Decisions in Romania - Balancing the Conflict between the Principle of Publicity in Court Proceedings and the Right to Personal Data Protection*, Jus et Civitas - A Journal of Social and Legal Studies vol. IV (LXVIII), no. 1/2017, p. 30-31.

[35] Article 3 of *Decision no. 884 of 20 August 2013* issued by the Plenary of the Superior Council of Magistracy, available at https://www.juridice.ro/wp-content/uploads/2015/06/16_09_2013__60647_ro.pdf.

legally binding decision of a supervisory authority concerning the data subjects, considering that there is no competent authority who could issue such a decision.

When data subjects consider that their rights derived from data protection have been infringed as a result of the processing of their personal data in non-compliance with Regulation (EU) 2016/679, the only means available to the plaintiff or the defendant in a Romanian civil suit is the right to an effective judicial remedy against the controller – namely the civil court that infringed, for instance, the data subjects' rights pursuant to articles 12 to 22 GDPR.

The lack of other remedies could be considered somewhat offset by the fact that all requests regarding the defence of the rights guaranteed by the General Data Protection Regulation are exempted from court stamp duty charges and the law provides an alternative territorial competence[36]. The competent court is that from the headquarters of the civil court – the controller – or from the habitual residence of the data subject, so it will be most convenient for the data subjects to exercise their rights in the latter jurisdiction.

Conclusions

Although the Code of Civil Procedure offers to data subjects such as the plaintiffs and the defendants the possibility to request that the civil proceedings are conducted without public presence, we cannot guess in what situations the court will actually consider that the publicity of the hearing could really affect the privacy of the parties. What we can say, however, is that the possible disclosure of sensitive data such as those regarding health or data concerning an individual's sex life or sexual orientation, should determine the court *ex officio* to declare the hearings closed to the general public.

Furthermore, since the decisions are usually delivered in public hearing, their reading should not include such sensitive data. Taking into account the protection of personal data and the protection of privacy, an example of good practice would be to postpone the decision and deliver it not in public hearing, but by making the solution available to the parties through the court clerk, in order to ensure, in particular, the principle of data minimisation. Also, as we already mentioned, civil courts could show a more proactive attitude towards their compliance with

[36] See article 8 (3) of *Annex I on the Procedure for receiving and resolving complaints* from the Decision of the President of the National Supervisory Authority for the Processing of Personal Data no. 133 from 3 July 2018, published in The Official Journal of Romania, Part I, no. 600 from 13 July 2018. According to article 3 (5) and (6) of Law no. 102 from 2 May 2005 on the establishment, organization and functioning of the National Supervisory Authority for the Processing of Personal Data, republished in The Official Journal of Romania, Part I, no. 947 from 9 November 2019, the said decision is normative and is mandatory for public authorities and institutions, private legal entities and any other bodies.

Regulation (EU) 2016/679 and request the implementation of technical measures to ensure *ex officio* the anonymisation of online data on the courts' portal concurrently with the physical archiving of the file.

Not least, in order to achieve a certain level of awareness among members of the judiciary of their obligations, civil courts should consider awareness-raising and training the staff involved in processing operations as part of the appropriate organisational measures taken in order to be able to demonstrate compliance with the General Data Protection Regulation.