N^0 251/2023

To the International Association of Judges – IAJ-UIM

The Romanian Magistrates' Association (AMR), professional and national, apolitical, non-governmental organization, stated to be of „public utility" through the Government Decision no. 530/2008 – with the headquarter in Bucharest, Regina Elisabeta Boulevard no. 53, District 5, e-mail amr@asociatia-magistratilor.ro, tax registration code 11760036 – legally represented by Judge dr. Andreea Ciucă - President, sends the following

ANSWERS TO THE SECOND STUDY COMMISSION QUESTIONNAIRE
"How data protection rules are impacting on the way judges work in civil litigation?"

1. In your jurisdiction is a court considered to be a data controller for data protection law purposes in all, or any, of the following situations:

a. When performing its judicial functions?
b. For purposes connected with the administration of justice, including the publication of a judgment or court decision, or a list or schedule of proceedings or of hearings in proceedings?
c. For purposes connected with the efficient management and operation of the courts and for statistical purposes?

The application, as of 25 May 2018, of Regulation (EU) 2016/679 has led to the need to harmonize national provisions with the provisions of the Regulation.

In this context, Law no. 129/2018 amending and supplementing Law no. 102/005 on the establishment, organization and functioning of the National Supervisory Authority for the Processing of Personal Data was mainly aimed at ensuring the powers and monitoring and control tasks of this authority, in accordance with Article 55-59 of Regulation (EU) 2016/679. In this way, the appropriate legal framework for the observance of the specific rights of individuals in the field of personal data processing has been ensured, as well as an effective interaction in the relationship between administration and citizens.

Each court is registered in the Register of personal data processing, managed by the National Supervisory Authority for the Processing of Personal Data. The courts process personal data for the purpose of exercising the duties provided for by law, in relation to the performance of judicial activity and other administrative activities (in particular those concerning human resources).

The application of Regulation (EU) 2016/679 at court level is part of the legislative framework which sets out their powers and duties. The processing of personal data by the courts is for the purpose of:

- ensuring access to justice
- ensuring access to public information and the right to petition
- carrying out the human resources activity
- monitoring/security of persons, premises and/or public/private property.

The persons concerned are: the parties in the cases, lawyers and legal representatives; representatives of central and local public authorities; petitioners and visitors; media representatives; court staff, gendarmes who guard the premises.

If the provision of personal data is a legal or contractual obligation or a necessary obligation to conclude a contract, the refusal to provide such data to the courts makes it impossible to settle the request addressed to the institutions, respectively the impossibility of concluding or performing the contract.

The methods of processing personal data by the courts are as follows:

- ♦ real-time video surveillance and image recording
- ♦ processing of data in paper format
- ♦ computerized data processing.

General information on the protection of personal data is published on the website of each court. Therefore, the public is informed of the general information relating to: *i)* the data that is published on the court portal, in relation to the cases registered before the court; *ii)* the fact that the court processes personal data in accordance with the provisions of Article 6 of (EU) Regulation 2016/679; *iii)* the fact that the individuals who do not want their first and last names to appear on the court portal must request this in writing to the court, the court being able to use, strictly from a technical point of view, the option of confidentiality when entering data in the ECRIS app, to remove them from the portal; *iv)* the fact that the data published on the courts' portal are automatically taken from the ECRIS app, according to the technical parameters of this application.

The ECRIS software has been implemented at national level since 2006. This software allows for each case:

- ✓ the verification of the registration date with the court,
- ✓ its object,
- ✓ stage of the procedure,
- ✓ the measures ordered by the court at each hearing,
- ✓ the date the decision is pronounced, the appeals filed,
- ✓ the date the file has been sent to the hierarchical superior court to deal with the appeal,
- ✓ the date the decision is pronounced,

- ✓ the date the file has been returned to be kept in the archives (in the first-degree court).

The courts, the Superior Council of Magistracy, the Judicial Inspection and the Ministry of Justice are all registered on the ECRIS software.

The data from the ECRIS software placed at the public's disposal are automatically displayed on the portal of each court.

By accessing the portal (www.portal.just.ro) the public may obtain information on:

- ❖ number and object of the case file,
- ❖ name of the parties (see exceptions below),
- ❖ date of registration with the court,
- ❖ date of last modification of the recorded data in the ECRIS software,
- ❖ the section of the court where the case was assigned,
- ❖ the stage of the procedure,
- ❖ the hearings that took place and measures ordered by the court (in short),
- ❖ the decision of the court (in short),
- ❖ the appeals which have been filed.

Courts have ownership of the databases in the ECRIS computer application and their content. The data are filled in by each court, according to the Internal Rules of the courts, approved by the Decision of the Section for judges of the Superior Council of Magistracy no. 3243/2022.

In the performance of judicial functions, the data published on the court portal (computer application at national level) are automatically taken from the databases of the ECRIS computer app managed by each court. Only the names and surname of the parties or the names of the files shall be published on the portal, provided that the data submitted are adequate, relevant and not excessive.

The data from the files in which the use of the "confidential" option was ordered are excluded from publication on the courts' portal. The "confidential" tick is applied in the ECRIS program when registering the file and is "inherited" when transferring the file electronically to the courts dealing with appeals.

The courts also use the function of anonymizing the name of the injured party in the criminal files having as their object one of the offenses established by Decision no. 600/2021 of the Section for Judges of the Superior Council of Magistracy (offenses committed against a family member, trafficking and exploitation of vulnerable persons and crimes against sexual freedom and integrity). In this case, the "protect personal data" tick is applied in the ECRIS program.

It should be noted that the function of anonymizing the name of the injured party can be used, in all cases, at the request of the injured party or its legal representative.

Also, the anonymization function (by ticking "protect personal data") can be used with regard to the name and surname or name of the party of any file, who requested in writing the anonymization, if the court orders this measure.

Individuals who do not want the files' data to be published on the portal of the courts of law must address the court handling the file in question. If the confidentiality option is ordered, it will be used to enter data in the ECRIS computer application, and in this way the data is also removed from the court portal.

The difference between the "confidential" option and the anonymization option ("protect personal data") is that, in the first case, no document on file can be seen on any electronic platform (not even in the "Electronic file" application intended for the parties and their lawyers). In the second case, the file documents can be seen on the portal of the courts, but the name and surname of the party who requested anonymity cannot be seen.

The data subject has the right to request the erasure of personal data concerning him or her for the following reasons: *a)* they are no longer necessary for the performance of the purposes for which they were collected or otherwise processed; *b)* there is no legal basis for the processing; *c)* the data subject objects to the processing and there are no overriding legitimate grounds; *d)* the personal data have been unlawfully processed; *e)* the personal data must be erased for compliance with a legal obligation.

2. In your jurisdiction does a data subject (e.g. a party to litigation, a witness, or a party whose interests may be affected by the litigation) have a right to information regarding the processing of their personal data by or on behalf of the courts?

The data subject has the right to obtain from the court a confirmation or denial of the processing of personal data and, in case of an affirmative answer, has the right to access such data and information on how the data are processed.

Anyway, as mentioned above, the processing of the personal data methods listed in the answer to question 1 are published on the portal of each court.

Also, on the courts' websites, information is published on the procedure to be followed by the persons who make requests regarding the protection of personal data. For example, it is noted that such requests addressed to the courts must be made in writing, must be dated and signed, that they can be submitted to the general court register or sent to the court's electronic mail address.

With regard to the information on the names of the parties in a file, it can be obtained by consulting the court portal, except where the option of confidentiality or the option of anonymization has been used (as indicated in the answer to the previous question).

3. In your jurisdiction does a data subject whose personal data is published in a court document such as a judgment, have the right to seek rectification of allegedly inaccurate or inappropriately disclosed personal data?

The data subject shall have the right to obtain, without undue delay, the rectification of inaccurate personal data concerning him or her or their completion.

For this purpose, the person must submit a written request to the court where the file is located. If it is found that the personal data of the data subject, which have been published, are inaccurate or incomplete, the request is admissible. As a result, inaccurate data will be corrected and incomplete data will be filled in immediately. These operations are carried out by the person in charge of entering in the ECRIS computer application the name and surname, respectively the name of the parties in each file.

4. In your jurisdiction is personal data contained in a judgment or decision of a court, or in a list or schedule of proceedings or hearings, generally made accessible to the public? If so, are there exceptions and what are they? If not, is there a redaction requirement, or alternative requirement, to be implemented before a judgment / list /schedule can be published so as to safeguard the rights of data subjects?

Data from the files registered in the ECRIS computer application of each court, including court decisions, are published on the internet, either on the courts' portal or via the case-law portal "ReJust".

As regards to the publication of judgments on the courts' portal, we mention that the personal data contained therein is protected by anonymization. In this regard, by Decision no. 37/2015, issued by the High Court of Cassation and Justice – The Panel for Preliminary Ruling on Questions of Law, it was established that the name and surname of a person represent information relating to personal data, regardless of whether, in a given situation, they are or not sufficient to identify the person.

The data and decisions given in the files in which the use of the "confidential" option was ordered are excluded from publication on the court's website. Also, the data and decisions given in files expressly excluded from publication by Decision no. 884/2013 of the Superior Council of

Magistracy are not published. For example, the data and decisions given in cases concerning minors and family, treason, espionage, rape, sexual intercourse with a minor, incest, child pornography, obligation to medical treatment, prohibition, invention patents, etc.

"ReJust" portal is an application designed and developed by the Superior Council of Magistracy. The portal was created for the following purposes:

- ❒ to enable citizens and specialists of the judiciary system to have easier access to decisions given by national courts;
- ❒ to improve knowledge of judicial practice in certain areas;
- ❒ to ensure greater transparency inside and outside the judiciary system;
- ❒ to improve access to justice by increasing information, awareness of citizens' rights and development of legal culture.

The decisions come from all courts, and any interested person can access decisions given at the level of all jurisdiction degrees.

The decisions in the ReJust Portal are anonymized and cannot be identified by the file number or by the names of the parties. Each document has a unique identification code, which can be used to cite the case-law and to verify the document's existence within the portal.

Regarding the personal data contained in the hearing lists (name and surname or name of the parties), we mention that, in case of files in which the use of the option "confidential" or the option "protect personal data" was ordered (see the distinctions in the answer to question 1), the name and surname or names of the parties are not published. Therefore, the name of either party does not appear in the hearing list on that file.

5. How are complaints addressed in your jurisdiction concerning alleged breaches by the courts of the rights of data subjects? Does your jurisdiction have a person or body with special responsibility for the supervision of data processing operations of courts when acting in their judicial capacity?

By Article 34 (2) of Law no. 305/2022 on the Superior Council of Magistracy, the role of the competent Authority Council was established for the supervision of the personal data processing operations of the courts in the exercise of their judicial powers, within the meaning of Article 55 (3) of (EU) Regulation 2016/679.

These provisions were issued in accordance with argument (20) and in relation to Article 55 (3) of the Regulation. In argument 20 of the Regulation, the following were noted:

"(...) 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. It 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".

According to art. 55 para 3 of the Regulation, *"Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity".*

Therefore, for the personal data processing activity carried out by the courts in the exercise of their judicial powers, the Superior Council of Magistracy is the institution with supervisory and control powers. Therefore, the Council has the duties of monitoring and verifying the personal data processing activity of the courts.

The data subject submits the request/complaint regarding the processing of personal data to the court where the file is located. There are two ways to record the request/complaint, depending on the path chosen by the data subject. If it is drafted in the file and filed/submitted to the general registry of the court, it is registered on file and handed over to the panel of judges to order. If the request/complaint is made based on the Law on free access to information of public interest, it is registered at the Information and Public Relations Office. The expert at this office shall refer it to the panel for order.

If the data subject considers himself or herself to be harmed by the response received or does not receive a response within the legal term to a request for the exercise of the rights provided for in Article 12-22 of the Regulation, addressed to a court, as a personal data controller, that person has the possibility to submit a complaint to the Superior Council of Magistracy.

According to Article 108 (1) of the Rules of Organization and Functioning of the Superior Council of Magistracy, the Personal Data Protection Department shall perform the necessary work for the performance of the role of the competent Authority Council to supervise the personal data processing operations of the courts in the exercise of their judicial duties.

In this regard, the Superior Council of Magistracy has the following powers:

i) Carries out duties to ensure that the courts comply with the rules laid down in (EU) Regulation 2016/679, namely:

- monitoring and enforcement by courts of the Regulation;
- carrying out verifications on the application of the Regulation;

- issuing warnings to the courts that the processing operations might violate the provisions of the Regulation;
- issuing provisions to the courts to comply with the requests of the data subject to exercise their rights under the Regulation;
- issuing provisions to the courts to ensure compliance of processing operations with the provisions of the Regulation, specifying, where appropriate, the manner and time limit for it;
- order the courts to inform the data subject of a personal data breach;
- imposition of temporary or definitive limitations, including prohibitions on processing, on certain categories of data;
- order the rectification or erasure of personal data or restriction of processing pursuant to Articles 16, 17 and 18 of the Regulation, as well as order the notification of such actions to the recipients to whom the personal data have been disclosed, in accordance with Articles 17(2) and 19 of the Regulation.

ii) Carries out duties to raise awareness among members of the judiciary system of their obligations under the Regulation:

- advising courts and preparing instructions on legislative and administrative measures relating to the protection of the rights and freedoms of natural persons with regard to processing;
- cooperation with the National Supervisory Authority for the Processing of Personal Data, to ensure consistency of application and compliance of the Regulation by the courts.

iii) Carries out duties regarding the settlement of complaints made by natural persons who consider that the processing by the courts, in the exercise of their judicial powers, of personal data concerning them violates the Regulation, case in which the Superior Council of Magistracy may make recommendations or may refer other competent authorities, as appropriate.

6. In your experience have data protection rules impacted adversely on your judicial independence? If so, how have they done so?

Our colleagues did not report any negative impact on the independence of the judge, either in general or in particular. Such an impact did not result either from the requests we are aware of, made by the parties concerned, regarding the processing of personal data. Also, the performance of the duties of the Superior Council of Magistracy, as an institution with supervisory and control powers for the personal data processing activity carried out by the courts, in the exercise of their judicial duties, has not had, so far, a negative impact on the independence of the judge.

Judge Andreea Ciucă, PhD
Romanian Magistrates' Association (AMR)